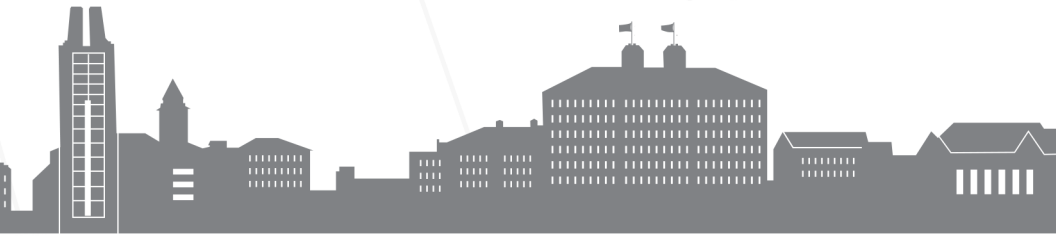
7TH ANNUAL

HOT TOPICS *in the* SCIENCE OF SECURITY

SEPTEMBER 22-24, 2020 | Virtually hosted by THE UNIVERSITY OF KANSAS

http://hotsos.org



virtually hosted by:

THE UNIVERSITY OF KANSAS

7TH ANNUAL

HOT TOPICS in the SCIENCE OF SECURITY

September 22-24, 2020

http://hotsos.org

WELCOME

Welcome to the 7th Annual Hot Topics in the Science of Security (HotSoS) Symposium, hosted by The University of Kansas after a several month COVID-19 delay. The goal of HoTSoS is to bring together researchers, practitioners, and thought leaders from government, industry, and academia, and to provide a forum for dialogue focused on developing and advancing scientic foundations in cybersecurity. The unique technical emphasis of HotSoS is building a foundational science of security. Specifically, incorporating scientific methods, data gathering and analysis, experimental approaches, mathematical models, and the interactions among them to create a scientific basis for security.

The symposium program will feature a mix of invited talks, presentations of refereed papers, a poster session, and work-in-progress (WiP) discussion sessions designed to provide authors and the security community with early, in-depth feedback on new unpublished research.

As in previous years, HotSoS 2020 focuses on problems related to:

- **Scalability and composability** in the construction of secure systems,
- **Policy-governed collaboration** for handling data across different domains of authority while ensuring security and privacy,
- **Security metrics** and improved **measurement tools**, to guide choice making in security engineering and response,
- **Resilient architectures** that can deliver service despite compromised components,
- **Analysis of human behavior,** encompassing users, operators, and adversaries, to support improved cybersecurity design.

Submissions were subject to a rigorous reviewing process, and ultimately 12 out of 17 papers submitted to the symposium were accepted, including one systemization of knowledge paper. In addition, 6 papers submitted to the special works-in-progress session were accepted. The program also includes 20 posters that will be presented during the poster session.

We are grateful to Joshua Guttman, Michael Hicks, Andrew Gacek, and Lyle Paczkowski for giving keynote talks at HoTSoS and we thank the members of the program committee for all their work. We thank Jason Hayden for helping with logistics and moving HoTSoS from April to September in one day. We would like to express our appreciation to Katie Dey for her outstanding support including managing the web site, interfacing with ACM, scheduling, and generally keeping us on the right path. Finally, we thank Adam Tagert and Heather Lucas for helping with conference organization and acknowledge the National Security Agency (NSA) for their continual support of the science of security community.

Drew Davidson & Baek-Young Choi - Program Chairs
Perry Alexander - General Chair

TABLE OF CONTENTS

INFORMATION

VIRTUAL PLATFORM:

The 2020 HotSoS symposium will be hosted on the Hopin virtual conferencing platform. Hopin is a virtual venue with multiple interactive areas that are optimized for connecting and engaging. The Symposium is free to attend but you must register to gain access:

http://hotsos.org/registration

POSTER SESSION:

A virtual poster session will take place on Tuesday, September 22 from 3:45 - 5:15 pm. The poster exhibition area will be open to browse throughout the conference. We will have a lightning session with 3-minute poster presentations from 3:45 to 4:45 pm. From 4:45 to 5:15 pm we will break into small groups for poster discussions.

SYMPOSIUM PRESENTATIONS:

Symposium presentations and posters will be available online at:

http://hotsos.org/agenda

SURVEY:

Please take a moment to respond to our short survey at:

http://hotsos.org/survey-2020

Your valuable feedback will help us plan future events.

POLICIES:

HotSoS is committed to providing a safe and enjoyable event experience for all participants, and a welcoming environment for free discussion of ideas. We do not tolerate harassment of participants in any form during events or in any HotSoS online space or social media. If you have any concerns about inappropriate behavior by any participant during the event, please contact the HotSoS organizers:

Email: hotsos2020@cps-vo.org
Hopin chat: send a message to Katie Dey

Please review the complete code of conduct at:

http://hotsos.org/policies

By participating in this event, you consent to having your audio and video recorded.

GENERAL CHAIR:

PERRY ALEXANDER is the AT&T Distinguished Professor of Electrical Engineering and Computer Science and Director of the Information and Telecommunication Technology Center at The University of Kansas. Dr. Alexander leads the KU Science of Security Lablet. His research interests include system-level modeling, design languages, heterogeneous specification, language semantics, and trusted computing. He received the BSEE and BSCS in 1986, the MSEE in 1988, and the PhD in 1992 all from The University of Kansas. From September 1992 through July 1999 he was a faculty member and Director of The Knowledge-Based Software Engineering Laboratory in the Electrical and Computer Engineering and Computer Science department at The University of Cincinnati. Dr. Alexander has been involved in numerous projects funded by DARPA, AFRL, NSF, NASA, NavAir, Battelle,and US Department of Defense. He currently leads the ACHILLES and ArmoredSoftware efforts at ITTC. He is the chief architect of the Rosetta system specification language and is author of System-Level Design using Rosetta. Dr. Alexander has published over 100 refereed research papers. He has won 22 teaching awards and was named a Kemper Teaching Fellow and the ASEE's Midwest Region Teacher of the Year in 2003, and received the Sharp Teaching Professorship in 2009. He is a member of Sigma Xi and a Senior Member of ACM and IEEE.

PROGRAM CO-CHAIRS:

BAEK-YOUNG CHOI is an Associate Professor in the Department of Computer Science Electrical Engineering at the University of Missouri – Kansas City. She received her PhD degree in Computer Science from the University of Minnesota. Her research interests lie in the broad areas of computer networks and systems including Smart Device Technologies, Internet-of-Things, Cloud, Network and Storage Management Systems, and Security. She published three books on network monitoring, storage systems, and cloud computing. She has been a faculty fellow of the National Aeronautics and Space Administration (NASA), U.S. Air Force Research Laboratory (AFRL), and Korea Telecom Advance Institute of Technology (KT-AIT). She is a senior member of ACM and IEEE, and a member of IEEE Women in Engineering.

DREW DAVIDSON is an Assistant Professor in the Department of Electrical Engineering and Computer Science at the University of Kansas. He received his MS and PhD degrees from the University of Wisconsin-Madison. Prior to his role at the University of Kansas, he worked as a founding engineer of Tala Security where he was the Principle Investigator of Small Business Innovation Research (SBIR) award from the NSF. His research focuses on the use of program analysis to detect and mitigate privacy and security issues in software. He is especially interested in work involving modern platforms such as mobile devices, autonomous vehicles, and cloud systems.

ORGANIZATION

PROGRAM COMMITTEE:

GUL AGHA, University of Illinois Urbana-Champaign
NIRAV AJMERI, North Carolina State University
EHAB AL-SHAER, University of North Carolina Charlotte
ALEXANDRU BARDAS, University of Kansas
ALVARO A. CÁRDENAS, University of California Santa Cruz
ERIC CLEMONS, National Security Agency
LORENZO DE CARLI, Worcester Polytechnic Institute
FENGJUN LI, University of Kansas
BO LUO, University of Kansas
VAIBHAV RASTOGI, University of Wisconsin Madison
ADAM TAGERT, National Security Agency

ORGANIZING COMMITTEE:

GENERAL CHAIR:
PERRY ALEXANDER, University of Kansas

PROGRAM CHAIRS:
BAEK-YOUNG CHOI, University of Missouri, Kansas City
DREW DAVIDSON, University of Kansas

NSA LIASONS:
HEATHER LUCAS and **ADAM TAGERT**

LOCAL ARRANGEMENTS CHAIR:
JASON HAYDON, University of Kansas

PUBLICITY CHAIR:
KATIE DEY, Vanderbilt University

MEETING ORGANIZERS:
ALEXIS RODRIGUEZ, Vanderbilt University
REGAN WILLIAMS, Vanderbilt University

GRAPHIC DESIGN:
AMY KARNS, Vanderbilt University

Tuesday, September 22

AGENDA

1000 - 1015 **Opening Remarks & Winning Paper Announcement**
Symposium Chairs: *Perry Alexander, Baek-Young Choi, and Drew Davidson*

NSA Opening Remarks

1015 - 1115 **Keynote: Access Control Verification for Everyone**
Andrew Gacek, Amazon Web Services

1115 - 1130 **Break**

PAPER SESSION 1: CPS and Industrial Control

(20 minutes per paper with 10 minutes of flex in the block)

1130 - 1300 **Simulation Testbed for Railway Infrastructure Security and Resilience Evaluation**
**Himanshu Neema, *Xenofon Koutsoukos, **Bradley Potteiger, †Cheeyee Tang, and †Keith Stouffer*
*Vanderbilt University, **Johns Hopkins APL, †National Institute of Standards and Technology

@PAD: Adversarial Training of Power Systems Against Denial of Service Attacks
Ali I Ozdagli, Carlos Barreto, and Xenofon Koutsoukos
Vanderbilt University

The More the Merrier: Adding Hidden Measurements for Anomaly Detection and Mitigation in Industrial Control Systems
**Jairo Giraldo, **David Urbina, †CheeYee Tang, and ††Alvaro Cárdenas*
*University of Utah, **University of Texas at Dallas, †National Institute of Standards and Technology, ††The University of California, Santa Cruz

RUCKUS: A Cybersecurity Engine for Performing Autonomous Cyber-Physical System Vulnerability Discovery at Scale
Bradley Potteiger, Jacob Mills, Daniel Cohen, and Paul Velez
*Johns Hopkins Applied Physics Laboratory

1300 - 1400 **Break**

WORKS IN PROGRESS (WiP) SESSION 1

1400 - 1530 ***Sohaib Kiani, *Fengjun Li, **Chao Lan, and *Bo Luo**
*University of Kansas, **University of Wyoming

Jacob Fustos, Michael Bechtel, and Heechul Yun
University of Kansas

1530 - 1545 **Break**

1545 - 1715 **Poster Session**

AGENDA

Wednesday, September 23

1000 - 1100 **KEYNOTE: Is Hardware Root of Trust hard to do, and Trustworthy?**
Lyle Paczkowski, Sprint

1100 - 1115 **Break**

PAPER SESSION 2: Modeling

(20 minutes per paper with 10 minutes of flex in the block)

1115 - 1245 **Exploring Hackers Assets: Topics of Interest as Indicators of Compromise**
Mohammad Al-Ramahi, Izzat Alsmadi, and Joshua Davenport
Texas A&M, San Antonio

Cyber Threat Modeling and Validation: Port Scanning and Detection
Eric Vugrin, Jerry Cruz, Christian Reedy, Thomas Tarman, and Ali Pinar
Sandia National Laboratories

Can We Use Software Bug Reports to Identify Vulnerability Discovery Strategies?
Farzana Ahamed Bhuiyan, Raunak Shakya, and Akond Rahman
Tennessee Technological University

Automated Influence and the Challenge of Cognitive Security
Sarah Rajtmajer and Daniel Susser
The Pennsylvania State University

1245 - 1345 **Break**

WORKS IN PROGRESS (WiP) SESSION 2

1345 - 1515 ***Hao Xue, *Qiaozhi Wang, *Bo Luo, **Chao Lan, *Fengjun Li**
*University of Kansas, **University of Wyoming

Ryan Karl, Jonathan Takeshita, and Taeho Jung
University of Notre Dame

1515 - 1530 **Break**

1530 - 1630 **Keynote: Trust Engineering with Cryptographic Protocols**
Joshua Guttman
Worcester Polytechnic Institute / MITRE

Thursday, September 24

AGENDA

1000 - 1100 **KEYNOTE: Evaluating Fuzz Testing (and other technologies)**
Michael Hicks
University of Maryland / Correct Computation, Inc.

1100 - 1115 **Break**

PAPER SESSION 3: Systems

(20 minutes per paper with 10 minutes of flex in the block)

1115 - 1245 **Neutralizing Manipulation of Critical Data by Enforcing Data-Instruction Dependency**
Chandra Sharma, Nathan Miller, and George Amariucai
Kansas State University

Ghostbusting: Mitigating Spectre with Intraprocess Memory Isolation
**Ira Ray Jenkins, *Prashant Anantharaman, **Rebecca Shapiro, *J Peter Brady, *Sergey Bratus, and *Sean W Smith*
*Dartmouth College, **Narf Industries

WOLF: Automated Machine Learning Workflow Management for various Applications
**Sohaib Kiani, *Sana Awan, **Jun Huan, **Fengjun Li, and *Bo Luo*
*University of Kansas, **StylingAI Inc

A Formal Security Analysis of ZigBee (1.0 and 3.0)
**Li Li, **Proyash Podder, and *Endadul Hoque*
*Syracuse University, **Florida International University

1245 - 1345 **Break**

WORKS IN PROGRESS (WiP) SESSION 3

1345 - 1515 **Tsion Yimer, Md Tanvir Arafin, and Kevin Kornegay**
Morgan State University

Sana Awan, Bo Luo, Fengjun Li
University of Kansas

1515 - 1530 **Break**

1530 - 1545 **Announcement of Winning Poster**
Adam Tagert

Closing Remarks
Perry Alexander, Baek-Young Choi, Drew Davidson, and Adam Tagert

Symposium Adjourned

KEYNOTE

Tuesday, September 22 @ 10:15 a.m.

ANDREW GACEK
Amazon Web Services

Access Control Verification for Everyone

Amazon Web Services (AWS) recently launched IAM Access Analyzer, an automated reasoning service for auditing permissions to cloud resources. While all customers want increased security, few have the specialized skills required to formally specify and verify security properties. Customers who go down this road have to formally specify their intended security properties, check them against their policies, and then debug when properties fail to hold. Access Analyzer inverts this situation: it quickly and automatically discovers security properties and then asks customers which ones are intended. This eliminates the skill barrier and upfront time costs associated with traditional formal verification. As a result, everyone can have formally verified security properties and the confidence that comes with them.

Andrew Gacek is a Senior Applied Scientist in the Automated Reason Group at Amazon Web Services. Andrew designs services that use automated reasoning to help customers secure their applications and data. Previously, Andrew worked at Rockwell Collins, building formal verification tools for certification of safety critical avionics systems. Andrew holds a PhD in Computer Science from the University of Minnesota.

Wednesday, September 23 @ 10:00 a.m.

LYLE PACZKOWSKI
Sprint

Is Hardware Root of Trust hard to do, and Trustworthy?

As the appetite for exploiting security flaws intensifies, so does the broad spectrum of vulnerabilities. It's important to consider each type of vulnerability and how these could impact physical or logical systems. This presentation will detail four areas of vulnerabilities and appropriate hardware and software methods with which to combat incursions and data larceny.

Lyle Paczkowski is a Senior Technology Strategist for Sprint's Advanced Technology Development division. A twenty five year innovative information technologies veteran, Mr. Paczkowski has 173 awarded patents on Security, Blockchain, Hardware Root of Trust, NFV, IMS, Network, 3G CDMA, 4G LTE, NFC, wireless access, and media application patent awards, and 58 patents pending. He has extensive experience in large-scale wireless infrastructure deployments, contact center solutions, application development and project management, and computerized telephony integration (CTI) technologies. He has been with Sprint for 22 years.

Mr. Paczkowski is also credited for the directing the development of several advanced enterprise wireless voice and media applications and products, including converged and integrated wireless and wireline applications. His field of work includes a unique mobile integration product known as Sprint Mobile Integration using IP Multimedia Subsystem (IMS). He has created new Near Field Communications applications, including co-inventing a new novel UHF RFID bar code replacement chip design (to be used in IoT appliances); wireless application development; Unified Communications enhancements; new hardware-assisted security protocols, and hosted multimedia platforms. Mr. Paczkowski presents at numerous domestic and international technology conferences as a subject matter expert focusing upon mobile network device security topics, Blockchain and Hyperledger protocols, and enterprise wireless converged application development. In the Telecom industry he is widely considered a "C-level" enterprise business and technology roadmap development expert.

He has a previous 13 year experience as a Senior Product Development Manager with Melroe/Ingersoll Rand responsible for the creation of several new construction equipment product lines, electronic order entry system development, and the deployment of a national construction equipment sales distribution strategy.

Mr. Paczkowski holds a bachelor degree in Economics from North Dakota State University. He is a US Army Veteran, married, and has two sons.

KEYNOTE

KEYNOTE

Wednesday, September 23 @ 3:30 p.m.

JOSHUA GUTTMAN
Worcester Polytechnic Institute / MITRE

Trust Engineering with Cryptographic Protocols

Dr. Joshua Guttman is a Senior Principal Scientist at the MITRE Corporation, and Research Professor at Worcester Polytechnic Institute. He has focused on security foundations and applications, including cryptographic protocol analysis and design, network security, operating systems security, and information flow. Dr. Guttman has written extensively, with about 75 academic publications, and regularly serves on program committees. He was educated at Princeton and the University of Chicago.

Thursday, September 24 @ 10:00 a.m.

MICHAEL HICKS
University of Maryland /
Correct Computation, Inc.

Evaluating Fuzz Testing (and other technologies)

Fuzz testing has enjoyed great success at discovering security critical bugs in real software. Researchers have devoted significant effort to devising new fuzzing techniques, strategies, and algorithms. Such new ideas are primarily evaluated experimentally so an important question is: What experimental setup is needed to produce trustworthy results? In mid 2018 we surveyed the research literature and assessed the experimental evaluations carried out by 32 fuzzing papers. We found problems in every evaluation we considered. We then performed our own extensive experimental evaluation using an existing fuzzer. Our results showed that the general problems we found in existing experimental evaluations can indeed translate to actual wrong or misleading assessments. We suggest that these problems can be avoided, thus making reported results more robust, by following some simple guidelines. Such guidelines are an instance of those developed subsequently by ACM SIGPLAN in an effort to improve the quality of empirical evaluations of automated testers, compilers, and analysis tools.

Michael W. Hicks is a Professor in the Computer Science department and the CTO of Correct Computation, Inc. He recently completed a three-year term as Chair of ACM SIGPLAN, the Special Interest Group in Programming Languages, and was the first Director of the University of Maryland's Cybersecurity Center (MC2). His research focuses on using programming languages and analyses to improve the security, reliability, and availability of software. He has explored the design of new programming languages and analysis tools for helping programmers find bugs and software vulnerabilities, and explored technologies to shorten patch application times by allowing software upgrades without downtime. Recently he has been looking at synergies between cryptography and programming languages, as well techniques involving random testing and probabilistic reasoning. He also led the development of a new security-oriented programming contest, "build-it, break-it, fix-it," which has been offered to the public and to students of his Coursera class on Software Security. He edits the SIGPLAN blog, PL Perspectives (https://blog.sigplan.org), and maintains his own blog, the PL Enthusiast, at http://www.pl-enthusiast.net/.

KEYNOTE

PAPER LISTING

Listed in order of program

Simulation Testbed for Railway Infrastructure Security and Resilience Evaluation
**Himanshu Neema, *Xenofon Koutsoukos, **Bradley Potteiger, †CheeYee Tang, †Keith Stouffer*
*Vanderbilt University, **Johns Hopkins AP Laboratory, †NIST

@PAD: Adversarial Training of Power Systems Against Denial-of-Service Attacks
Ali I Ozdagli, Carlos Barreto, Xenofon Koutsoukos
Vanderbilt University

The More the Merrier: Adding Hidden Measurements to Secure Industrial Control Systems
**Jairo Giraldo, **David Urbina, †CheeYee Tang, ††Alvaro A. Cárdenas*
University of Utah, University of Texas at Dallas, †NIST, ††University of California, Santa Cruz

RUCKUS: A Cybersecurity Engine for Performing Autonomous Cyber-Physical System Vulnerability Discovery at Scale
Bradley Potteiger, Jacob Mills, Daniel Cohen, Paul Velez
Johns Hopkins University Applied Physics Laboratory

Exploring Hackers Assets: Topics of Interest as Indicators of Compromise
Mohammad Al-Ramahi, Izzat Alsmadi, Joshua Davenport
Texas A&M University

Cyber Threat Modeling and Validation: Port Scanning and Detection
Eric D. Vugrin, Jerry Cruz, Christian Reedy, Thomas Tarman, Ali Pinar
Sandia National Laboratories

PAPER LISTING

Can We Use Software Bug Reports to Identify Vulnerability Discovery Strategies?
Farzana Ahamed Bhuiyan, Raunak Shakya, Akond Rahman
Tennessee Technological University

Automated Influence and the Challenge of Cognitive Security
Sarah Rajtmajer and Daniel Susser
The Pennsylvania State University

Neutralizing Manipulation of Critical Data by Enforcing Data-Instruction Dependency
Chandra Sharma, Nathan Miller, George Amariucai
Kansas State University

Ghostbusting: Mitigating Spectre with Intraprocess Memory Isolation
**Ira Ray Jenkins, *Prashant Anantharaman, **Rebecca Shapiro, *J. Peter Brady, *Sergey Bratus, *Sean W. Smith*
*Dartmouth College, **Narf Industries

WOLF: Automated Machine Learning Workflow Management Framework for Malware Detection and other applications
**Sohaib Kiani, *Sana Awan, **Jun Huanz, *Fengjun Li, and *Bo Luo*
*University of Kansas, **StylingAI Inc

A Formal Security Analysis of ZigBee (1.0 and 3.0)
**Li Li, **Proyash Podder, *Endadul Hoque*
*Syracuse University, **Florida International University

Simulation Testbed for Railway Infrastructure Security and Resilience Evaluation

**Himanshu Neema, *Xenofon Koutsoukos, **Bradley Potteiger,*
†CheeYee Tang, †Keith Stouffer
*Vanderbilt University, **Johns Hopkins Applied Physics Laboratory, †NIST

Himanshu Neema is a Research Assistant Professor of Computer Science at Vanderbilt University. He holds a M.S. and Ph.D. in Computer Science from Vanderbilt University. Dr. Neema researches in the general area of model-based design and modeling and simulation of Cyber-Physical Systems and their integrated simulation with hardware- and humans- in the loop. His research interests include: Model-Based Design, Cyber-Physical Systems, Distributed Simulations & Analysis of System-of-Systems, Heterogeneous Simulation Integration, Cybersecurity, Risk Analysis, Network Simulation, Scenario-Based Experimentation, Cloud Computing, Big Data, Resilient Systems, Design Automation, Design Space Exploration, Artificial Intelligence, Machine Learning, Adversarial Machine Learning, Constraint Programming, Planning & Scheduling, Resource Allocation, Constraint Solving, Operations Research, Service-Oriented Architectures, Blockchains, Smart-Grids, Transactive Energy, Smart Cities. Dr. Neema has 22 years of experience in research and development of software applications covering above areas and has co-authored more than 50 publications. He is the creator of the model-based simulation integration and rapid experimentation framework called Cyber-Physical Systems Wind Tunnel (CPSWT), which has been recently successfully transitioned to the US National Institute of Standards and Technology (NIST).

Abstract:

The last decade has seen an influx of digital connectivity, operation automation, and remote sensing and control mechanisms in the railway domain. The management of the railway operations through the use of distributed sensors and controllers and with programmable and remotely controllable railway signals and switches has led to gains in system efficiency as well as operational flexibility. However, the network connectivity has opened up the railway cyber communication networks to cyber-attacks. These are a class of cyber-physical systems (CPS) with interconnected physical, computational, and communication components. The cyber-attacks on these systems could potentially cascade through these interconnection and result into significant damage. These systems are safety-critical owing to their large-scale monetary and, more importantly, human life safety concerns. Therefore, it is better to incorporate security and resilience requirements right from the design time. In this paper, we describe a domain-specific framework for simulations in the railway domain. The framework allows analyzing the resilience of railway operations in the presence of cyber-attacks. In particular, our simulation framework allows modeling the railway network as well as the railway transportation. It provides an online graphical modeling environment that allows multiple users to collaborate, through a web-based interface, over the same model for the railway infrastructure as well as network attacks. The framework also allows the user to configure and run experiments through the web-interface and also to visualize the key operational

metrics from the railway domain as the experiment is running. The framework also supports executing large simulations in the cloud. In addition, it supports hardware-in-the-loop (HIL) simulation for incorporating physical effects and network attacks that can only be realized realistically in the hardware. A detailed case study is provided to demonstrate the framework's capabilities.

@PAD: Adversarial Training of Power Systems Against Denial-of-Service Attacks

Ali I Ozdagli, Carlos Barreto, Xenofon Koutsoukos
Vanderbilt University

Ali Irmak Ozdagli is a graduate student in the Department of Electrical Engineering and Computer Science at Vanderbilt University. His research focuses on security and resilience of cyber-physical systems. Contact him at ali.i.ozdagli@vanderbilt.edu.

Carlos Barreto is a postdoctoral scholar at Vanderbilt University. His research interests include security and resiliency of cyber-physical systems, risk analysis, and game theoretic analysis of security problems. He received the Ph.D. in computer science from the University of Texas at Dallas. He is member of the IEEE. Contact him at carlos.a.barreto@vanderbilt.edu.

Xenofon Koutsoukos is a professor with the department of electrical engineering and computer science and a senior research scientist with the Institute for Software Integrated Systems, Vanderbilt University. His research work is in the area of cyber-physical systems with emphasis on security and resilience, control, diagnosis and fault tolerance, formal methods, and adaptive resource management. He received the Ph.D. degree in electrical engineering from the University of Notre Dame. He is a Fellow of the IEEE. Contact him at xenofon.koutsoukos@vanderbilt.edu.

Abstract:

In this work, we study the vulnerabilities of protection systems that can detect cyber-attacks in power grid systems. We show that machine learning-based discriminators are not resilient against Denial-of-Service (DoS) attacks. In particular, we demonstrate that an adversarial actor can launch DoS attacks on specific sensors, render their measurements useless and cause the attack detector to classify a more sophisticated cyber-attack as a normal event. As a result of this, the system operator may fail to take action against attack-related faults leading to a decrease in the operation performance. To realize a DoS attack, we present an optimization problem to determine which sensors to attack within a given budget such that the existing classifier can be deceived. For linear classifiers, this optimization problem can be formulated as a mixed-integer linear programming problem. In this paper, we extend this optimization problem to find attacks for more complex classifiers such as neural networks. We demonstrate that a neural network, in particular, with RELU activation functions, can be represented as a set of logic formulas using Disjunctive Normal Form, and the optimization problem can be used to efficiently compute a DoS attack. In addition, we propose a defense model that improves the resilience of neural networks against DoS through adversarial training. Finally, we evaluate the efficiency of the approach using a dataset for classification in power systems.

The More the Merrier: Adding Hidden Measurements to Secure Industrial Control Systems

**Jairo Giraldo, **David Urbina, †CheeYee Tang, ††Alvaro A. Cárdenas*
University of Utah, University of Texas at Dallas, †NIST,
††University of California, Santa Cruz

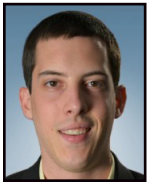
Alvaro A. Cárdenas is an Associate Professor of Computer Science and Engineering at the University of California, Santa Cruz. Before this, he was the Eugene McDermott Associate Professor of Computer Science at the University of Texas at Dallas. He was also a postdoctoral scholar at the University of California, Berkeley, and a research staff at Fujitsu Laboratories. He holds M.S. and Ph.D. degrees from the University of Maryland, College Park and a B.S. from Universidad de Los Andes. His research interests focus on cyber-physical systems and IoT security and privacy. He is the recipient of the NSF CAREER award, the 2018 faculty excellence in research award from the Erik Johnson School of Engineering and Computer Science, the Eugene McDermott Fellow Endowed Chair at the University of Texas at Dallas, and he is the receipient of best paper awards from the IEEE Smart Grid Communications Conference and the U.S. Army Research Conference, and a finalist of the CSAW competition in Israel.

Abstract:

Industrial Control Systems (ICS) collect information from a variety of sensors throughout the process, and then use that information to control some physical components. Control engineers usually have to pick which measurements they are going to use and then they purchase sensors to take these measurements. However, in most cases they only need a small subset of all possible measurements that can be used. Economic and efficiency reasons motivate engineers to use only a small number of sensors for controlling a system; however, as attacks against industrial systems continue to increase, we need to study a systematic way to add sensors to the system to identify potentially malicious attacks. We propose the addition of hidden sensor measurements to a system to improve its security. Hidden sensor measurements are by our definition measurements that were not considered in the original design of the system, and are not used for any operational reason. We only add them to improve the security of the system and using them in anomaly detection and mitigation. We show the addition of these new, independent, but correlated measurements to the system makes it harder for adversaries to launch false-data injection stealthy attacks and, even if they do, it is possible to limit the impact caused by those attacks. When an attack is detected, we replace the compromised sensor measurements with estimated ones from the new sensors improving the risky open-loop simulations proposed by previous work.

RUCKUS: A Cybersecurity Engine for Performing Autonomous Cyber-Physical System Vulnerability Discovery at Scale

Bradley Potteiger, Jacob Mills, Daniel Cohen, Paul Velez
Johns Hopkins University Applied Physics Laboratory



Dr. Bradley Potteiger is a current senior professional staff member and embedded exploitation researcher at The Johns Hopkins University Applied Physics Laboratory working within the Institute for Assured Autonomy and APL Asymmetric Operations Sector on cutting edge applications related to cybersecurity, space systems, election integrity and national security. He has also worked in the Executive Office of the President, The White House and has been supported by the NSA throughout his PhD studies. Dr. Potteiger received his Ph.D. from the Department of Electrical Engineering at Vanderbilt University and his B.S. Degree in Computer Engineering from the University of Maryland, Baltimore County. His dissertation focuses on creating a moving target defense (MTD) architecture for embedded devices to enhance CPS integrity, while maintaining availability with safe, reliable, and predictable system operations.

Abstract:

In 2016, the Cyber Grand Challenge (CGC) provided key foundations and motivations for navigating towards an autonomous cybersecurity approach. Since that time, novel strides have been made in the areas of static analysis, vulnerability discovery, patching, and exploit generation. However, a majority of these efforts have been focused on enterprise systems, leaving a gap in the Cyber-Physical System (CPS) domain. With the rise of connected infrastructure and the introduction of 5G communications, CPS are becoming more ingrained within present-day society. Due to a large amount of legacy software, and control of safety-critical actuation, CPS are and will continue to be a huge attack vector for our adversaries to remotely deploy devastating attacks against our country with low economic cost and at scale. To combat this threat, we propose the need to apply the most beneficial concepts from the CGC to create more secure and resilient CPS. In this paper, we introduce a CPS security assessment architecture RUCKUS for autonomously identifying and analyzing CPS firmware, identifying vulnerabilities, and developing exploits. Further, our approach considers how to integrate graph analytics to extrapolate findings to firmware at scale, allowing for measuring the potential widespread impact of attacks. Our architecture is demonstrated using an automotive case study, leveraging firmware from the most popular automotive and router manufacturers to assess the real-world potential impact of CPS attacks.

Exploring Hackers Assets: Topics of Interest as Indicators of Compromise

Mohammad Al-Ramahi, Izzat Alsmadi, Joshua Davenport
Texas A&M University

Izzat Alsmadi is an Assistant Professor in the department of computing and cyber security at the Texas A&M, San Antonio. He has his master and PhD in Software Engineering from North Dakota State University in 2006 and 2008. He has more than 100 conference and journal publications. His research interests include: Cyber intelligence, Cyber security, Software security, software engineering, software testing, social networks and software defined networking. He is lead author, editor in several books including: Springer The NICE Cyber Security Framework Cyber Security Intelligence and Analytics, 2019, Practical Information Security: A Competency-Based Education Course, 2018, Information Fusion for Cyber-Security Analytics (Studies in Computational Intelligence), 2016. The author is also a member of The National Initiative for Cybersecurity Education (NICE) group, which meets frequently to discuss enhancements on cyber security education at the national level.

Abstract:

The need to develop actionable intelligence that is proactive is very critical to current security controls and systems. Hackers and hacking techniques continue to grow and become more sophisticated. As such Security teams start to adopt proactive and offensive approaches within hackers' territories. In this scope, we proposed a systematic approach to automatically extract "topics of interest, ToI" from hackers' websites. Those can eventually be used as inputs to actionable security controls or Indicators of Compromise (IOS) collectors. As a showcase, we selected the hackers' news website "CrackingFire". ToI can be integrated into Indicators of Compromise (IoC) and once correlated with other signs of attacks from those IoC will trigger further cybersecurity offense or defense actions. We also developed our own dark web crawler and evaluate extracting ToIs. We observed the types of challenges in both the crawling and the processing stages.

Cyber Threat Modeling and Validation: Port Scanning and Detection

Eric D. Vugrin, Jerry Cruz, Christian Reedy, Thomas Tarman, Ali Pinar
Sandia National Laboratories

Eric Vugrin is a Distinguished Member of Technical Staff at Sandia National Laboratories in Albuquerque, New Mexico. His current research focuses on modeling and analyzing the resilience of industrial control systems and other critical infrastructure. His work has provided research, operational, and policy guidance to the U.S. Department of Energy, the U.S. Department of Homeland Security, the U.S. Department of Defense, and other federal agencies. He received his PhD in Mathematics from Virginia Tech.

Abstract:

Port scanning is a commonly applied technique in the discovery phase of cyber attacks. As such, defending against them has long been the subject of many research and modeling efforts. Though modeling efforts can search large parameter spaces to find effective defensive parameter settings, confidence in modeling results can be hampered by limited or omitted validation efforts.

In this paper, we introduce a novel, mathematical model that describes port scanning progress by an attacker and intrusion detection by a defender. The paper further describes a set of emulation experiments that we conducted with a virtual testbed and used to validate the model. Results are presented for two scanning strategies: a slow, stealthy approach and a fast, loud approach. Estimates from the model fall within 95% confidence intervals on the means estimated from the experiments. Consequently, the model's predictive capability provides confidence in its use for evaluation and development of defensive strategies against port scanning.

Can We Use Software Bug Reports to Identify Vulnerability Discovery Strategies?

Farzana Ahamed Bhuiyan, Raunak Shakya, Akond Rahman
Tennessee Technological University

Raunak Shakya is a graduate student at the Department of Computer Science, Tennessee Technological University, currently working towards a MS in Computer Science. He graduated with a Bachelor's degree in Engineering from Institute of Engineering, Tribhuvan University, Nepal in 2013. Then he worked as a software developer for more than three and a half years in various software companies based in my hometown Kathmandu, Nepal. His areas of interest include (but not limited to) software engineering, machine learning, data analysis, web application development and business and finance.

Abstract:

Daily horror stories related to software vulnerabilities necessitates the understanding of how vulnerabilities are discovered. Identification of data sources that can be leveraged to understand how vulnerabilities are discovered could aid cybersecurity researchers to characterize exploitation of vulnerabilities. The goal of the paper is to help cybersecurity researchers in characterizing vulnerabilities by conducting an empirical study of software bug reports. We apply qualitative analysis on 729, 908, and 5336 open source software (OSS) bug reports respectively, collected from Gentoo, LibreOffice, and Mozilla to investigate if bug reports include vulnerability discovery strategies i.e. sequences of computation and/or cognitive activities that an attacker performs to discover vulnerabilities, where the vulnerability is indexed by a credible source, such as the National Vulnerability Database (NVD). We evaluate two approaches namely, text feature-based approach and regular expression-based approach to automatically identify bug reports that include vulnerability discovery strategies.

We observe the Gentoo, LibreOffice, and Mozilla bug reports to include vulnerability discovery strategies. Using text featurebased prediction models, we observe the highest prediction performance for the Mozilla dataset with a recall of 0.78. Using the regular expression-based approach we observe recall to be 0.83 for the same dataset. Findings from our paper provide the groundwork for cybersecurity researchers to use OSS bug reports as a data source for advancing the science of vulnerabilities.

Automated Influence and the Challenge of Cognitive Security

Sarah Rajtmajer and Daniel Susser
The Pennsylvania State University

Sarah Rajtmajer is an assistant professor in the College of Information Sciences and Technology and research associate in the Rock Ethics Institute at The Pennsylvania State University. Before joining the Penn State faculty, she served as a consultant to the Defense Advanced Research Projects Agency on scientific programs aimed at breakthrough technologies for national security, with specific focus on initiatives in big data and computational social science. Prior to her work in consulting, Dr. Rajtmajer was an Intelligence Community Postdoctoral Research Fellow at the Applied Research Laboratory and a Postdoctoral Scholar in the Department of Mathematics at Penn State.

Dr. Rajtmajer has a PhD in Mathematics from the University of Zagreb, Croatia, and a BA in Mathematics from Columbia University.

Daniel Susser is an assistant professor in the College of Information Sciences and Technology and a research associate in the Rock Ethics Institute at The Pennsylvania State University. A philosopher by training, Daniel works at the intersection of technology, ethics, and policy. His research aims to highlight normative issues in the design, development, and use of digital technologies, and to clarify conceptual issues that stand in the way of addressing them through law and policy. At the moment, he's especially focused on questions about privacy, online influence, and automated decision-making. Daniel received his PhD in philosophy from Stony Brook University and BA in computer science and philosophy from the George Washington University.

Abstract:

Advances in AI are powering increasingly precise and widespread computational propaganda, posing serious threats to national security. The military and intelligence communities are starting to discuss ways to engage in this space, but the path forward is still unclear. These developments raise pressing ethical questions, about which existing ethics frameworks are silent. Understanding these challenges through the lens of "cognitive security," we argue, offers a promising approach.

Neutralizing Manipulation of Critical Data by Enforcing Data-Instruction Dependency

Chandra Sharma, Nathan Miller, George Amariucai
Kansas State University

Chandra Sharma got his BS degree in Computer Engineering from Kathmandu Engineering College in 2015.

As a graduate student at Kansas State University since 2017, his research is mostly focused on software security and information security. One of his active research is on finding the optimal trade-off between privacy and utility of the information shared by users on the internet. His another research work is focused on developing novel techniques to protect against code-injection and code-reuse attacks. Some of his other research interests includes vehicular security and application of game theory to information security.

Abstract:

In this paper, we propose a new approach to neutralize attacks that tamper with critical program data. Our technique uses a sequence of instructions as a trap against the illicit modification of the critical data. In a nutshell, we set up a dependency such that the continued execution of the program is contingent upon the successful execution of the instruction sequence and the successful execution of the instruction sequence is contingent upon the integrity of the critical data. In particular, we discuss a specific implementation of our technique focusing on a critical data that is often subject to malicious manipulation: the return address of a function. We show that our technique can be an effective countermeasure to defend against attacks that overwrite the return address to divert control to a malicious code. We further show that our technique offers significant protection without resorting to complementary defenses such as ASLR, DEP or StackGuard.

Ghostbusting: Mitigating Spectre with Intraprocess Memory Isolation

**Ira Ray Jenkins, *Prashant Anantharaman, **Rebecca Shapiro, *J. Peter Brady, *Sergey Bratus, *Sean W. Smith*
*Dartmouth College, **Narf Industries

Prashant Anantharaman is a Ph.D. student at Dartmouth College who works on Language-Theoretic Security. He works on securing various Industrial IoT and Power Grid protocols by building secure parsers for them and has recently begun exploring various binary file and protocol formats.

Abstract:

Spectre attacks have drawn much attention since their announcement. Speculative execution creates so-called transient instructions, those whose results are ephemeral and not committed architecturally. However, various side-channels exist to extract these transient results from the microarchitecture, e.g., caches. Spectre Variant 1, the so-called Bounds Check Bypass, was the first such attack to be demonstrated. Leveraging transient read instructions and cachetiming effects, the adversary can read secret data.

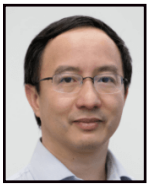
In this work, we explore the ability of intraprocess memory isolation to mitigate Spectre Variant 1 attacks. We demonstrate this using Executable and Linkable Format-based access control (ELFbac) which is a technique for achieving intraprocess memory isolation at the application binary interface (ABI) level. Additionally, we consider Memory Protection Keys (MPKs), a recent extension to Intel processors, that partition virtual pages into security domains. Using the original Spectre proof-of-concept (POC) code, we show how ELFbac and MPKs can be used to thwart Spectre Variant 1 by constructing explicit policies to allow and disallow the exploit. We compare our techniques against the commonly suggested mitigation using serialized instructions, e.g., lfence. Additionally, we consider other Spectre variants based on transient execution that intraprocess memory isolation would naturally mitigate.

WOLF: Automated Machine Learning Workflow Management Framework for Malware Detection and other applications

**Sohaib Kiani, *Sana Awan, **Jun Huan, *Fengjun Li, and *Bo Luo*
*University of Kansas, **StylingAI Inc

Sohaib Kiani is currently a PhD-Computer Science candidate in University of Kansas. His research interests include Adversarial Machine Learning and applications of machine learning algorithms for various security applications. He did his MS in Information Technology from RWTH Aachen, Germany and BS in Communication Engineering from NU-FAST Islamabad, Pakistan.

Sana Awan is currectly a PhD-Computer Science Candidate in University of Kansas. Her area of research is Cybersecurity, particularly security in the Internet of Things domain. She designed and implemented network security solutions and intrusion detection systems that employ machine learning to improve security while maintaining reliability and continued deployment. She did her MS in System Engineering from University of Maryland, USA and BS in Electrical Engineering from NUST Islamabad, Pakistan.



Dr. Jun (Luke) Huan is the Chief Scientist and Chief Executive Officer of Styling.AI, a start-up providing AI services to the fashion industry. Before that he served as a Distinguished Scientist and the Head of Big Data Lab at Baidu Inc : From 2006-2018 he served as the Charles and Mary Jane Spahr Professor in the Department of Electrical Engineering and Computer Science at the University of Kansas. From 2015 to 2018, he served as a Program Director for the US National Science Foundation, in charge of the Big Data Program of NSF.

Dr. Fengjun Li is an associate professor at the Department of Electrical Engineering and Computer Science of the University of Kansas. She received B.E. degree (with honor) from the University of Science and Technology of China in 2001, M.Phil. from the Chinese University of Hong Kong in 2004 and Ph.D. from the Pennsylvania State University in 2010. She received the Kansas NSF EPSCoR First Award in 2014, KU Miller Scholar Award in 2016 and KU Bellows Scholar Award in 2019. Her research interests lie in a broad area of security and privacy for distributed information systems, cyber-physical systems and communication networks.

Dr. Bo Luo is currently a full professor with the EECS department at the University of Kansas. He is the director of the Information Assurance Laboratory (IAL) at KU's Information and Telecommunication Technology Center (ITTC), which is a National Center of Academic Excellence in Cyber Defense designated by NSA and DHS. He was awarded the Miller Professional Development Award at KU in 2015, and the Miller Scholar awards in 2016 and 2017. He received Ph.D. degree from The Pennsylvania State University in 2008, M.Phil degree from the Chinese University of Hong Kong in 2003, and B.E. from University of Sciences and Technology of China in 2001.

Abstract:

Applying machine learning techniques to solve real-world problems is a highly iterative process. The process from idea to code and then to experiment may require up to thousands of iterations to find the optimum set of hyper-parameters. Also, it is hard to find best machine learning techniques for a given dataset. The WOLF framework has been designed to simultaneously automate the process of selecting the best algorithm and searching for the optimum hyper-parameters. It can be useful to both who are novice in machine learning and just want to find best algorithm for their dataset, and also to those who are experts in the field and want to compare their new features or algorithm with state of the art techniques. By incorporating the WOLF framework in their designs, it is easier for novices to apply machine learning techniques on their dataset. With a wide range of evaluation metrics provided, WOLF also helps data scientists to develop better intuition towards machine learning techniques and speed up the process of algorithm development. Another main feature of the WOLF framework is that user can easily integrate new algorithms at any stage of the machine learning pipeline. In this paper, we present the WOLF architecture, and demonstrate how it could be used for standard machine learning datasets and for Android malware detection tasks. Experimental results show the flexibility and performance of WOLF.

A Formal Security Analysis of ZigBee (1.0 and 3.0)

**Li Li, **Proyash Podder, *Endadul Hoque*
*Syracuse University, **Florida International University

Li Li is a graduate student in the Department of Electrical Engineering and Computer Science at Syracuse University. His research interests span over computer and IoT systems security, network security, and privacy-preserving protocols.

Abstract:

The rapid increase in the number of IoT devices in recent years indicates how much financial investment and efforts the tech-industries and the device manufacturers have put in. Unfortunately, this aggressive competition can give rise to poor quality IoT devices that are prone to adversarial attacks. To make matter worse, these attacks can compromise not only security but also safety, since an IoT device can directly operate on the physical world. Many recently reported attacks are due to the insecurity present in the underlying communication protocol stacks, and ZigBee is one of them. Considering the emergence and adoption of ZigBee 3.0 and the current market share of ZigBee 1.0, it is essential to study and analyze these protocol stacks at their specification level so that any insecurity at the specification level should be identified and fixed before they go into production.

With that goal in mind, in this paper, we develop a model for ZigBee (1.0 and 3.0) and reason about its security properties using a security protocol verification tool (named Tamarin). Our model of ZigBee closely follows the ZigBee specification, and the security properties are derived from the ZigBee specification. We use Tamarin to verify these properties on our model and report our findings on ZigBee 1.0 and ZigBee 3.0.

POSTER LISTING

A Curated Dataset of Security Defects in Scientific Software Projects
Justin Murphy, Elias T. Brady, Shazibul Islam Shamim, Akond Rahman
Tennessee Technological University

A Preliminary Taxonomy of Techniques Used in Software Fuzzing
Raunak Shakya and Akond Rahman
Tennessee Technological University

A Raspberry Pi Sensor Network for Wildlife Conservation
Andrew Arnold, Paul Corapi, Michael Nasta, Kevin Wolgast, Thomas A. Babbitt
United States Military Academy

Accelerating Block Propagation in PoW Blockchain Networks with Pipelining and Chunking
Kaushik Ayinala, Baek-Young Choi, Sejun Song
University of Missouri - Kansas City

An Infrastructure for Faithful Execution of Remote Attestation Protocols
Adam Petz
University of Kansas

An seL4-based Architecture for Layered Attestation
Grant Jurgensen, Michael Neises, Perry Alexander
University of Kansas

An Uncertain Graph-based Approach for Cyber-security Risk Assessment
Hoang Hai Nguyen
University of Illinois at Urbana-Champaign

Application of the Armament Cyber Assessment Framework
Aidan McCarthy, Liam Furey, Keagan Smith, Daniel Hawthorne, Raymond Blaine
United States Military Academy

Building a Conceptual Framework for Ethical Hacking
Lauren E. Provost, Rebecca Labitt, Danielle Alexandre, Asher Rodriguez
Simmons University

Decentralized Backup and Recovery of TOTP Secrets
Conor Gilsenan, Noura Alomar, Andrew Huang, Serge Egelman
University of California, Berkeley

Do Configuration Management Tools Make Systems More Secure? An Empirical Research Plan
Md Rayhanur Rahman, William Enck, Laurie Williams
North Carolina State University

Listed alphabetically

Exploiting DRAM Bank Mapping and HugePages for Effective Denial-of-Service Attacks on Shared Cache in Multicore
Michael Bechtel and Heechul Yun
University of Kansas

How to Swap Instructions Midstream: An Embedding Algorithm for Program Steganography
Ryan Gabrys, Luis Martinez, Sunny Fugate
Naval Information Warfare Center

Improving Architectures for Automating Network Security Using Specification-Based Protocols
Khir Henderson and Kevin Kornegay
Morgan State University

Resilient Multi-Robot Target Pursuit
Jiani Li, Waseem Abbas, Mudassir Shabbir, Xenofon Koutsoukos
Vanderbilt University

Time Series Anomaly Detection in Medical Break-the-Glass
Qais Tasali, Nikesh Gyawali, Eugene Y. Vasserman
Kansas State University

Tokens of Interaction: Psycho-physiological Signals, A Potential Source of Evidence of Digital Incidents
Nancy Mogire
University of Hawaii at Manoa

Toward Just-in-Time Patching for Containerized Applications
Olufogorehan Tunde-Onadele, Yuhang Lin, Jingzhu He, Xiaohui Gu
North Carolina State University

Using Intel SGX to Improve Private Neural Network Training and Inference
Ryan Karl, Jonathan Takeshita, Taeho Jung
University of Notre Dame

Vulnerability Trends in Web Servers and Browsers
**M S Raunak, **Richard Kuhn, *Richard Kogut, **Raghu Kacker*
*Loyola University Maryland, **NIST

POSTER LISTING

A Curated Dataset of Security Defects in Scientific Software Projects

Justin Murphy, Elias T. Brady, Shazibul Islam Shamim, Akond Rahman
Tennessee Technological University

Justin Murphy is an Undergraduate Student at Tennessee Technological University. He is a senior fast-track student studying Computer Science concentrating in Cybersecurity and a CyberCorps Scholarship for Service (SFS) recipient. His research interests are in Software Security, Software Analytics, and DevOps.

A Preliminary Taxonomy of Techniques Used in Software Fuzzing

Raunak Shakya and Akond Rahman
Tennessee Technological University

Raunak Shakya is a graduate student at the Department of Computer Science, Tennessee Technological University, currently working towards a MS in Computer Science. He graduated with a Bachelor's degree in Engineering from the Institute of Engineering, Tribhuvan University, Nepal in 2013. Then he worked for around four years as a software developer in various software companies based in his hometown Kathmandu, Nepal, before moving to the USA in 2019 to pursue further studies. His areas of interest include, but not limited to, software engineering, machine learning, data analysis, web application development, and finance and economics.

A Raspberry Pi Sensor Network for Wildlife Conservation

Andrew Arnold, Paul Corapi, Michael Nasta, Kevin Wolgast, Thomas A. Babbitt
United States Military Academy

Andrew Arnold is a cadet at the United States Military Academy. He is earning his undergraduate degree in Computer Science. He has branched Medical Service and will serve as a medical evacuation pilot.

Paul Corapi is a cadet at the United States Military Academy. He is earning his undergraduate degree in Computer Science. He has branched Aviation and will serve as a pilot in the Army.

Michael Nasta is a cadet at the United States Military Academy. He is earning his undergraduate degree in Electrical Engineering. He has branched Cyber and will serve as an officer in the Army.

Kevin Wolgast is a cadet at the United States Military Academy. He is earning his undergraduate degree in Computer Science. He has branched Engineers and will serve as an officer in the Army.

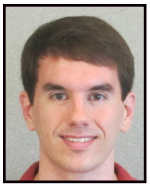
Accelerating Block Propagation in PoW Blockchain Networks with Pipelining and Chunking

Kaushik Ayinala, Baek-Young Choi, Sejun Song
University of Missouri - Kansas City

Kaushik Ayinala is a Ph.D. student of Computer Networks and Communication Systems department at the University of Missouri - Kansas City. He did his bachelor's in computer science engineering at GITAM university in India. He is currently working on the scalability problems of blockchain. His research interests include IoT, Blockchain, Cloud Computing, System designing.

An Infrastructure for Faithful Execution of Remote Attestation Protocols

Adam Petz
University of Kansas



Adam Petz is a PhD student in Computer Science at the University of Kansas under the guidance of his advisor, Dr. Perry Alexander. Adam's broad research interests include formal methods, programming language semantics, functional programming, trusted computing, and computer security. Adam has contributed to a number of successful externally-funded research projects while at the University of Kansas, and is currently working under the Cyber Assured Systems Engineering(CASE) DARPA effort. Adam completed his Master's in Computer Science at the University of Kansas in 2016, and completed two B.S. degrees in Computer Science and Mathematics at Emporia State University in 2014.

An seL4-based Architecture for Layered Attestation

Grant Jurgensen, Michael Neises, Perry Alexander
University of Kansas

Grant Jurgensen is a Master's student at the University of Kansas, working under Dr. Perry Alexander. His research interests include formal methods, secure systems, and programming languages. He has primarily worked on the DARPA Cyber Assured Systems Engineering (CASE) project, building secure components and architecture for remote attestation.

An Uncertain Graph-based Approach for Cyber-security Risk Assessment

Hoang Hai Nguyen
University of Illinois at Urbana-Champaign

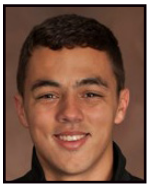
Hoang Hai Nguyen (Frank) is a Ph.D. candidate in the Department of Electrical and Computer Engineering at the University of Illinois at Urbana-Champaign (UIUC). He also holds a research assistantship at the Coordinated Science Laboratory, UIUC, under the direction of professor David M. Nicol. Before joining UIUC, he worked for four years as a full-time software engineer at the Advanced Digital Sciences Center (ADSC), a Singapore-based research center established and led by UIUC. He got his Bachelor of Computing degree in Computer Engineering (with honours) from the School of Computing, National University of Singapore (NUS) in 2011. His research interest is security modeling and analysis of networked computer systems, risk assessment applied to network security, and simulation of cyber-physical systems. His current work is supported by the National Security Agency's Science of Security (SoS) project and the Electric Power Research Institute (EPRI).

Application of the Armament Cyber Assessment Framework

Aidan McCarthy, Liam Furey, Keagan Smith,
Daniel Hawthorne, Raymond Blaine
United States Military Academy

Aidan McCarthy is a senior at the United States Military Academy from Lexington, Massachusetts. He is majoring in Computer Science with a focus in cybersecurity. He is an OSCP and leads the Cadet Competitive Cyber Team. After graduation, Aidan will commission as an officer in the United States Army Cyber Corps.

Liam Furey is a senior at the United States Military Academy from Cape Cod, Massachusetts. He is majoring in Computer Science with a focus in cyber policy. He leads the West Point Cyber Policy Team, taking them to an international championship in 2019. After graduation, Liam will commission as an officer in the United States Army Cyber Corps.



Keagan Smith is a senior at the United States Military Academy from Huntley, Illinois. He is majoring in Computer Science with a focus in network security. Keagan is CCENT Certified and am NCAA collegiate track athlete. After graduation, Keagan will commission as an officer in the United States Army Signal Corps.

Building a Conceptual Framework for Ethical Hacking

Lauren E. Provost, Rebecca Labitt, Danielle Alexandre, Asher Rodriguez
Simmons University

Rebecca Labitt will be graduating from Simmons University in December 2020. She is a computer science major with a passion for cybersecurity, and is excited to pursue a career in this field.

Danielle Alexandre is a Junior at Simmons University. She is majoring in Information Technology but is also interested in formal methods, especially in relation to cybersecurity.

Asher Rodriguez is a Senior at Simmons University, also working in industry in government in the area of cybersecurity.

Decentralized Backup and Recovery of TOTP Secrets

Conor Gilsenan, Noura Alomar, Andrew Huang, Serge Egelman
University of California, Berkeley

Conor Gilsenan is a doctoral student in Computer Science at the University of California, Berkeley. His research encompasses usable security and privacy and he is specifically interested in building tools to help people overcome the inherent usability challenges in authentication and account recovery systems. Prior to commencing research as a member of the Berkeley Lab for Usable and Experimental Security (BLUES), Gilsenan spent a decade in industry working as a software engineer.

Do Configuration Management Tools Make Systems More Secure? An Empirical Research Plan

Md Rayhanur Rahman, William Enck, Laurie Williams
North Carolina State University

Md Rayhanur Rahman has started his Ph.D. program in the department of Computer Science at North Carolina State University. His research interest is in the area of Software Engineering and Software Security. He works under the supervision of Dr. Laurie Williams. Currently he is working on the research domain of mining the cyber threat intelligence artifacts. He has received his bachelor's and master's degree in Software Engineering at University of Dhaka, Bangladesh.

Exploiting DRAM Bank Mapping and HugePages for Effective Denial-of-Service Attacks on Shared Cache in Multicore

Michael Bechtel and Heechul Yun
University of Kansas

Michael Bechtel is a Computer Science Ph.D. student at the University of Kansas. His current research interests include embedded real-time systems, microarchitectural security and machine learning applications. He earned an Outstanding Paper Award at RTAS 2019 for his work on denial-of-service (DOS) attacks on shared cache in embedded multicore systems. Michael received a B.S. degree in Computer Science from the University of Kansas in 2017.

How to Swap Instructions Midstream: An Embedding Algorithm for Program Steganography

Ryan Gabrys, Luis Martinez, Sunny Fugate
Naval Information Warfare Center

Ryan Gabrys is a scientist at the Naval Information Warfare Center Pacific. His research interests include theoretical computers science with applications to cyber security and information storage.

Improving Architectures for Automating Network Security Using Specification-Based Protocols

Khir Henderson and Kevin Kornegay
Morgan State University

Khir Henderson is a Doctor of Engineering candidate (D.Eng) at Morgan State Univesity located in Baltimore Maryland under the guidance of his advisor Kevin Kornegay. He also serves as a Graduate Researcher in the Center for Reverse Engineering and Applied Microelectronics Lab (CREAM) also under the advisement of Dr. Kevin Korneday. He also works part time for the Johns Hopkins Applied Physics Lab as a GEM fellow contributing to cybersecurity systems research. His current research is on the Cyber/Network security of embedded systems concerning the Internet of Things.

Resilient Multi-Robot Target Pursuit

Jiani Li, Waseem Abbas, Mudassir Shabbir, Xenofon Koutsoukos
Vanderbilt University

Jiani Li is currently working toward the Ph.D. degree with the Electrical Engineering and Computer Science Department, Vanderbilt University, Nashville, TN, USA. Her research focuses on resilient concensus, learning and optimization in multi-agent distributed systems and resilient design of cyber-physical systems with machine learning components.

Time Series Anomaly Detection in Medical Break-the-Glass

Qais Tasali, Nikesh Gyawali, Eugene Y. Vasserman
Kansas State University

Qais Tasali is a Ph.D candidate at Kansas State University. His doctoral research is focused on access control in medical cyber-physical systems. He is also interested in computer communications (networks), distributed computing and information security. Qais is a Fulbright alumnus and has a master of software engineering (MSE) degree from Kansas State University. Prior to graduate work, he worked as an IT director at Kabul University, working to develop sustainable IT for public universities in cooperation with German Academic Exchange Program (DAAD) and NATO Science Projects (Silk-way) in Afghanistan.

Nikesh Gyawali is a Computer Engineer and worked as a Security Analytics Engineer for two years at LogPoint, a SIEM solution. His interest lies in the field of intersection of Artificial Intelligence/Machine Learning and Cybersecurity. He is currently a Computer Science PhD student at Kansas State University.

Eugene Vasserman is an Associate Professor in the Department of Computer Science at Kansas State University, specializing in the security of distributed systems. He is also the director of the Kansas State University Center for Information and Systems Assurance. His current research is chiefly in the area of security for medical cyber-physical systems, security usability, and user education. His past work spans the gamut from security vulnerabilities emergent from the BGP infrastructure of the internet, to energy depletion attacks in low-power systems, to secure hyper-local social networking, to privacy and censorship resistance on a global scale (systems capable of supporting up to a hundred billion users). In 2013, he received the NSF CAREER award for work on secure next-generation medical systems.

He spent the 2016-2017 academic year on sabbatical at the FDA, serving as a security subject matter expert, taking regulator certification classes, and organizing and running a public workshop focused on regulatory science gaps in the way medical device security is handled. He has served on numerous program committees, including USENIX Security, ACSAC, PETS, USEC, ASIACCS, HotWiSec, WPES, SecureComm, and chaired the 2014 USENIX HealthTech Summit. He is a member of the UL 2900 standardization process for cybersecurity of network-connectable devices, the AAMI interoperability working group, and the AAMI / UL 2800 standards effort for medical device interoperability.

Tokens of Interaction: Psycho-physiological Signals, A Potential Source of Evidence of Digital Incidents

Nancy Mogire
University of Hawaii at Manoa

Nancy Mogire is a PhD candidate at UH Manoa's information and computer sciences department, affiliated with the Hawaii Interdisciplinary Neurobehavioral & Technology Lab(HINTLab) and the Adaptive Security and Economics Lab(ASECOLab). Previously, she earned an MSc. in Computer Science at the department.

Her dissertation work is focused on the psycho-physiological signal artifacts of human-computer interaction(HCI), and their potential applications towards solving cybersecurity problems.

Aside from research, she's a graduate teaching assistant in the computer science program at UH Manoa. She has spent the bulk of my TA time in courses related to computing security but also TA'd a variety of other courses including Algorithms, Software Engineering and Mobile Application Design.

Outside of curricular activities, she volunteers on various organizations that promote education in science and technology, with particular interest in programs that are focused on improving the welfare of women and marginalized groups in the society. Roles she has served in this regard include: Reviewing conference paper submissions, conducting phone interviews, chairing conference sessions and assisting with event logistics.

Toward Just-in-Time Patching for Containerized Applications

Olufogorehan Tunde-Onadele, Yuhang Lin, Jingzhu He, Xiaohui Gu
North Carolina State University

Olufogorehan (Fogo) Tunde-Onadele is a PhD student at North Carolina State University (NCSU) with research interests in Machine Learning and Security. He received his B.S. degree in Computer Engineering and M.S. degree in Computer Science from NCSU in 2017 and 2019, respectively. Fogo was a summer intern with Samsung Semiconductor, Inc. in 2019.

Yuhang Lin is a Ph.D. student at North Carolina State University with interests in Security, Artificial Intelligence and Systems. He received his B.S. degree in Mathematics from Zhejiang Normal University and M.S. degree in Computer Science from the University of Vermont in 2016 and 2018, respectively.

Jingzhu He is a Ph.D. student at North Carolina State University with interests in Distributed Systems, Cloud Computing and Big Data Analytics. She received her B.S. degree from the School of Electronic and Science Engineering of Nanjing University in 2013 as well as her M.Phil. degree from Hong Kong Baptist University in 2016. Jingzhu was a summer intern with Visa Research in 2019.

Xiaohui Gu is a full Professor in the Department of Computer Science at North Carolina State University.

She received her Ph.D. degree in 2004 and M.S. degree in 2001 from the Department of Computer Science, University of Illinois at Urbana-Champaign. She received her B.S. degree in Computer Science from Peking University, Beijing, China in 1999. She was a research staff member at IBM T. J. Watson Research Center, Hawthorne, New York, between 2004 and 2007.

She received the ILLIAC fellowship, David J. Kuck Best Master Thesis Award, and Saburo Muroga Fellowship from University of Illinois at Urbana-Champaign. She also received the IBM Invention Achievement Awards in 2004, 2006, and 2007.

She has filed nine patents, and has published more than 60 research papers in international journals and major peer-reviewed conference proceedings. She is a recipient of the NSF Career Award, four IBM Faculty Awards 2008,

2009, 2010, 2011, and two Google Research Awards 2009, 2011, best paper awards from ICDCS 2012 and CNSM 2010, and NCSU Faculty Research and Professional Development Award. She served as program co-chair for IEEE/ACM IWQoS 2013 and USENIX ICAC 2014. She is an associate editor for IEEE Transactions for Parellel and Distributed Systems (TPDS). She is a Senior Member of IEEE and a member of ACM.

Using Intel SGX to Improve Private Neural Network Training and Inference

Ryan Karl, Jonathan Takeshita, Taeho Jung
University of Notre Dame

Ryan Karl is a 3rd year graduate student in the Department of Computer Science and Engineering at The University of Notre Dame. He is broadly interested in Theoretic/Applied Cryptography and Computer Security, and focuses on leveraging trusted computing platforms to provide practical solutions to problems in Secure Multiparty Computation and Deep Learning. He holds a B.S. in Mathematics from Saint Vincent College.

Taeho Jung is an assistant professor of Computer Science and Engineering at the University of Notre Dame. He received the Ph.D. from Illinois Institute of Technology in 2017 and B.E. from Tsinghua University in 2011. His research area includes data security, user privacy, and applied cryptography. His paper has won a best paper award (IEEE IPCCC 2014), and two of his papers were selected as best paper candidate (ACM MobiHoc 2014) and best paper award runner up (BigCom 2015).

Raghu Kacker is a mathematical statistician in the Mathematical and Computational Sciences Division (MCSD) of the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). He received his Ph.D. in statistics from the Iowa State University. His research interests include evaluation of uncertainty in physical and virtual measurements, quantification of uncertainty from bias, combining information from interlaboratory evaluations and multiple methods of measurement, combinatorial methods, software vulnerability trends, and software quality testing and engineering.

He is a Fellow of the American Statistical Association and a Fellow of the American Society for Quality. He was an elected member of the International Statistical Institute. He has received Bronze medal from the U.S. Department of Commerce and Distinguished Technical Staff Award from the AT&T Bell Laboratories. He was member of an NIST team that developed software to assay large parallel processing programs, which won R&D 100 award. He is a member of the editorial boards of the journals Total Quality Management and Journal of Applied Statistics.

WiP LISTING

Listed alphabetically

Detecting Bots via Surrounding Neighborhoods
**Hao Xue, *Qiaozhi Wang, *Bo Lou, **Chao Lan, *Fenjun Li*
*University of Kansas, **University of Wyoming
Discussant: *Lorenzo De Carli*, Worcester Polytechnic Institute

DETGEN: Adversarial Detection using Partially Generated Images
**Sohaib Kiani, *Fengjun Li, **Chao Lan, *Bo Luo*
*University of Kansas, **University of Wyoming
Discussant: *Vaibhav Rastogi*, Google

Securing Industrial Control Systems using Physical Device Fingerprinting
Tsion Yimer, Md Tanvir Arafin and Kevin Kornegay
Morgan State University
Discussant: *Alvaro A. Cardenas*, University of California Santa Cruz

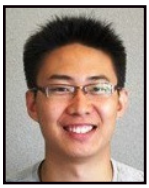
SpectreRewind: Leaking Secrets to Past Instructions
Michael Bechtel, Jacob Fustos, Heechul Yun
University of Kansas
Discussant: *Drew Davidson*, University of Kansas

Towards Privacy-Preserving Federated Transfer Learning for IoT
Sana Awan, Fengjun Li and Bo Luo
University of Kansas
Discussant: *Michael Branicky*, University of Kansas

Using Intel SGX to Improve Private Neural Network Training and Inference
Ryan Karl, Jonathan Takeshita and Taeho Jung
University of Notre Dame
Discussant: *Ahmad Ridley*, Department of Defense

Detecting Bots via Surrounding Neighborhoods

***Hao Xue**, *Qiaozhi Wang, *Bo Lou, **Chao Lan, *Fenjun Li*
*University of Kansas, **University of Wyoming



Hao Xue graduated from the University of Kansas and got his PhD Degree in Computer Science in Aug 2019. During his PhD program, his research interests are online spam review detection and information security.

DETGEN: Adversarial Detection using Partially Generated Images

***Sohaib Kiani,** *Fengjun Li, **Chao Lan, *Bo Luo*
*University of Kansas, **University of Wyoming*

Sohaib Kiani is currently a PhD-Computer Science candidate in University of Kansas. His research interests include Adversarial Machine Learning and applications of machine learning algorithms for various security applications. He did his MS in Information Technology from RWTH Aachen, Germany and BS in Communication Engineering from NU-FAST Islamabad, Pakistan.

Securing Industrial Control Systems using Physical Device Fingerprinting

***Tsion Yimer**, Md Tanvir Arafin and Kevin Kornegay*
Morgan State University

Tsion Yimer graduated from the University of Kansas and got his PhD Degree in Computer Science in Aug 2019. During his PhD program, his research interests are online spam review detection and information security.

SpectreRewind: Leaking Secrets to Past Instructions

Michael Bechtel, *Jacob Fustos, Heechul Yun*
University of Kansas

Michael Brechtel is a Computer Science Ph.D. candidate at the University of Kansas. His current research interests include Real-Time Systems, Embedded Systems, and Machine Learning. He received a B.S. in Computer Science from the University of Kansas in 2017.

Towards Privacy-Preserving Federated Transfer Learning for IoT

Sana Awan, *Fengjun Li and Bo Luo*
University of Kansas

Sana Awan is currectly a PhD-Computer Science Candidate at the University of Kansas. Her area of research is Cybersecurity, particulary security in the Internet of Things domain. She designed and implemented network security solutions and intrusion detection systems that employ machine learning to improve security while maintaining reliability and continued deployment. She did her MS in System Engineering from University of Maryland, USA and BS in Electrical Engineering from NUST Islamabad, Pakistan.

Using Intel SGX to Improve Private Neural Network Training and Inference

Ryan Karl, *Jonathan Takeshita and Taeho Jung*
University of Notre Dame

Ryan Karl is a 4th year graduate student in the Department of Computer Science and Engineering at The University of Notre Dame. He is broadly interested in Theoretic/Applied Cryptography and Computer Security, and focuses on leveraging trusted computing platforms to provide practical solutions to problems in Secure Multiparty Computation, Secure Aggregation, and Machine Learning. He holds a B.S. in Mathematics from Saint Vincent College.

HOTSOS BEST PAPER & POSTER AWARDS

The Best Paper and Poster Awards at HotSoS recognize cybersecurity research with scientific rigor, clarity of presentation, and global impact. These awards encourage scientists across multiple disciplines to address the fundamental problems of security in a principled manner.

http://sos-vo.org/competitions

BEST SCIENTIFIC CYBER-SECURITY PAPER COMPETITION

TThe Best Scientific Cybersecurity Paper Competition is sponsored by the NSA Research Directorate to promote rigorous research methods by identifying and highlighting excellence in science of security and privacy research. The competition accepts nominations from the public for refereed papers published in the previous year without geographic limitations. Nominated papers are evaluated by a panel of distinguished experts in cybersecurity. Winners are invited to NSA for recognition and to present their research.

http://sos-vo.org/papercompetition

NSA RESEARCH DIRECTORATE AWARD AT ISEF

The Annual Intel International Science and Engineering Fair (ISEF) is the world's largest international pre-college science competition with approximately 1,800 high school students from more than 75 countries, regions, and territories. To qualify, students must first win coveted spots from regions or countries. The Science of Security and Privacy Initiative has sponsored a special Science of Security award at the ISEF to recognize outstanding scientific accomplishment in cybersecurity and to encourage future generations of students to pursue cybersecurity education, research and careers.

http://sos-vo.org/ISEF

ANNUAL REPORT

The Science of Security and Privacy Annual Report details the progress of the activities in the Science of Security and Privacy research initiative. For more information about the activities associated with the SoS initiative, browse the SoS Annual Report on the SoS-VO.

https://cps-vo.org/sosannualreport

SOS-VO.ORG

The Science of Security Virtual Organization (SoS-VO) was established to provide a focal point for information about ongoing activities related to cybersecurity science and as a repository for significant research results. A major goal of all the Lablets is the creation of a unified body of knowledge that can serve as the basis of a cybersecurity discipline, curriculum, and rigorous design methodologies. The results of the SoS Lablet research are extensively documented and widely distributed through the SoS-VO.

SCIENCE OF SECURITY LABLETS

The NSA SoS Initiative has funded foundational multidisciplinary research at leading universities, promoted the growth of the community doing relevant research, and supported the adoption of scientific research methods. They stimulate basic research, create scientific underpinnings for security, advocate for scientific rigor in security research, and create and broaden a Science of Security community and culture. With an emphasis on building a community, each Lablet create partnerships with other universities called Sub-Lablets. Science of Security researchers freely collaborate with researchers in other institutions worldwide.

The Lablets work on making scientific advances in the 5 Hard Problems including Privacy, and Cyber-Physical Systems (CPS).

Currently Funded Research Lablets are Carnegie Mellon University, International Computer Science Institute, The University of Kansas, North Carolina State University, University of Illinois at Urbana-Champaign, and Vanderbilt University.

THE SCIENCE OF SECURITY 5 HARD PROBLEMS

The 5 Hard Problems are the broad research focus areas of SoS. These five were selected for their level of technical challenge, their potential operational significance, and potential benefit to research through the emphasis of scientific research methods. The five are not intended to be all inclusive of everything that needs to be done in cybersecurity but rather five specific areas that need scientific progress.

Scalability and Composability: Develop methods to enable the construction of secure systems with known security properties from components with known security properties, without a requirement to fully re-analyze the constituent components.

Policy-Governed Secure Collaboration: Develop methods to express and enforce normative requirements and policies for handling data with differing usage or privacy needs among users in different authority domains.

Security Metrics Driven Evaluation, Design, Development, and Deployment: Develop security metrics and models capable of predicting whether or confirming that a given cyber system preserves a given set of security properties (deterministically or probabilistically) in a given context.

Resilient Architectures: Develop means to design and analyze system architectures that deliver required services in the face of compromised components.

Understanding and Accounting for Human Behavior: Develop models of human behavior (of both users and adversaries) that enable the design, modeling, and analysis of systems with specified security properties.

APPLYING THE SOS HARD PROBLEMS

Within SoS, Privacy Foundations and Cyber-Physical Systems (CPS) have growing cyber impact, and are unique in application. SoS's CPS research examines the 5 Hard Problems in the context of CPS where the boundary between the cyber-domain and the physical world meet. SoS's Privacy research studies foundational privacy research challenges. Goals include a principled and methodological approach to evaluating privacy risk, and improving transparency.

sos-vo.org