

6TH ANNUAL
HOT TOPICS *in the* **SCIENCE OF SECURITY**

APRIL 1-3, 2019 | NASHVILLE, TENNESSEE

http://hot-sos.com



hosted by:

VANDERBILT UNIVERSITY

2019HoTSoSBooklet_revised.indd 1 3/18/19 10:48 AM





6TH ANNUAL

HOT TOPICS in the **SCIENCE OF SECURITY**

April 1-3, 2019 | Nashville, TN

http://hot-sos.com




WELCOME

Welcome to the 6th Annual Hot Topics in the Science of Security (HotSoS) Symposium and Bootcamp! The symposium will include a mix of invited talks, tutorials, presentations of refereed papers, a panel, a work in progress/work already published session, a poster session, and a special workshop session with the goal of providing the authors and the security community with early, in-depth feedback on new unpublished research.

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 centered upon the development and advancement of scientific foundations in cybersecurity. The technical emphasis of HotSoS lies on building a foundational science of security, incorporating scientific methods, data gathering and analysis, experimental approaches, mathematical models, and the interactions among them. The HotSoS vision is one of engaging and growing a community.

As in previous years, HotSoS 2019 specifically 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 7 out of 13 papers submitted to the symposium were accepted, and in addition 3 papers out of 8 papers submitted to the special workshop session were accepted. The program includes one tutorial, and 5 work in progress/work already published presentations. The program also includes 21 posters that will be presented during the poster session in both days. The theme of the poster session this year is security and privacy metrics and measurement techniques.

We are grateful to Rebecca Wright, Kevin Hamlen, and Trent Jaeger for giving keynote talks at HoTSoS, and to Tiffany Bao, Dan Geer, and Jonathan Spring for participating in the panel. We thank the members of the program committee for all their work. We would especially like to express our appreciation to Katie Dey for her exceptional help throughout this entire process, including handling logistics, managing the web site, and interfacing with ACM. To Adam Tagert for helping us with the conference organization, and for leading the panel. We would also like to thank Travis Breaux who chaired the new session discussing in-depth early work from unpublished manuscripts. Finally, we acknowledge the National Security Agency (NSA) for their continual support of the science of security community.

Alvaro A. Cardenas & Ehab Al-Shaer - Program Chairs
Xenofon Koutsoukos - General Chair

2019HoTSoSBooklet_revised.indd 2 3/18/19 10:48 AM

TABLE OF CONTENTS

Welcome 2

Table of Contents 3

General Information 4

Organization 5

Program Agenda 7

Keynote Bios 11

Poster Listing 14

SoS Outreach 16

Local Restaurants 18

Notes 19

2019HoTSoSBooklet_revised.indd 3 3/18/19 10:48 AM

INFORMATION

REGISTRATION:

Registration is located in the foyer of the Wyatt Center at Vanderbilt University. The registration desk is open during the following times:

6:00 p.m. to 7:30 p.m. Monday
8:00 a.m. to 5:30 p.m. Tuesday
8:00 a.m. to 4:30 p.m. Wednesday

WIRELESS INTERNET CONNECTION:

A wireless Internet connection is available on a hidden SSID.

Network Name: vummiv
Select "Join Other Network" and type vummiv.

SYMPOSIUM DINNER:

The symposium banquet will be held at The Bridge on Tuesday, April 2 at 6:30 p.m. Located on the riverfront downtown, this historic landmark originally served as an office building for Arthur Dyer's Nashville Bridge Company (NABRICO).

Venue Address:
2 Victory Avenue
Nashville, TN 37213

Parking is available in Lot R directly in front of The Bridge Building. The typical fare for an Uber/Lyft from midtown is less than $10.

POSTER SESSION:

Poster sessions will be be held in the Wyatt Rotunda during the following times:

Tuesday, April 2: 2:15 p.m. - 3:00 p.m.
Wednesday, April 3: 9:30 a.m. -10:15 a.m.

SYMPOSIUM PRESENTATIONS:

Symposium presentations and posters will be available online at:

http://hot-sos.com/agenda

SURVEY:

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

http://hot-sos.com/survey

Your valuable feedback will help us plan future events.

By participating in this event, you consent to having your image captured by official photographers and videographers. The resulting materials, including still photographs, video and audio recordings may be used by organizers without restriction or financial compensation, in news materials, promotional materials, and on the web.

2019HoTSoSBooklet_revised.indd 4 3/18/19 10:48 AM

GENERAL CHAIR:

XENOFON KOUTSOUKOS is a professor of Computer Science, Computer Engineering, and Electrical Engineering in the Department of Electrical Engineering and Computer Science at Vanderbilt University. He is also a Senior Research Scientist in the Institute for Software Integrated Systems (ISIS). Before joining Vanderbilt in 2002, Koutsoukos was a Research Staff Member in the Xerox Palo Alto Research Center, working in the Embedded Collaborate Computing Area. Between 1993 and 1995, he joined the National Center for Space Applications, Hellenic Ministry of National Defense, Athens, Greece as a computer engineer in the areas of image processing and remote sensing. Koutsoukos's research work is in the area of cyber-physical systems with emphasis on formal methods, distributed algorithms, diagnosis and fault tolerance, and adaptive resource management. He has published numerous journal and conference papers and he is co-inventor of four US patents. Professor Koutsoukos is the principal investigator of the Vanderbit University Science of Security Lablet.

PROGRAM CO-CHAIRS:

ALVARO CARDENAS is a Eugene McDermott Associate Professor of Computer Science at the University of Texas at Dallas. He holds M.S. and Ph.D. degrees from the University of Maryland, College Park. Before joining UT Dallas he was a postdoctoral scholar at the University of California, Berkeley, and a research staff at Fujitsu Laboratories of America in Sunnyvale California. 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 recognition at the University of Texas at Dallas, and best paper awards from the IEEE Smart Grid Communications Conference and the U.S. Army Research Conference.

EHAB AL-SHAER is a Professor and the Director of the Cyber Defense and Network Assurability (CyberDNA) Center in the School of Computing and Informatics at University of North Carolina Charlotte. His primary research areas are network security, security management, fault diagnosis, and network assurability. Prof. Al-Shaer edited/co-edited more than 10 books and book chapters, and published about 100 refereed journals and conferences papers in his area. Prof. Al-Shaer is the General Chair of ACM Computer and Communication 2009-2010 and NSF Workshop in Assurable and Usable Security Configuration, August 2008. Prof. Al-Shaer received his MSc and Ph.D. in Computer Science from the Northeastern University (Boston, MA) and Old Dominion University (Norfolk, VA) in 1998 and 1994 respectively.

2019HoTSoSBooklet_revised.indd 5 3/18/19 10:48 AM

ORGANIZATION

PROGRAM COMMITTEE:

YASEMIN ACAR, Leibniz University Hannover
JONATHAN ALDRICH, Carnegie Mellon University
PERRY ALEXANDER, University of Kansas
ALEXANDRU BARDAS, University of Kansas
NAZLI CHOUCRI, Massachusetts Institute of Technology
OMAR CHOWDHURY, University of Iowa
DANIELA CRUZES, SINTEF
ANDREW EMMS, National Cyber Security Centre
WILLIAM ENCK, North Carolina State University
SACHA FAHL, Ruhr-University Bochum
MARIA FERNANDEZ, Kings College London
ANAND GAJPARA, National Cyber Security Centre
DAVID GARLAN, Carnegie Mellon University
HELEN GU, North Carolina State University
KEVIN HAMLEN, University of Texas at Dallas
NIU JIANWEI, University of Texas San Antonio
KEVIN JIN, Illinois Institute of Technology
APU KAPADIA, Indiana University
CARL LANDWEHR, Cyber Pack Ventures, Inc.
ARON LASZKA, University of Houston
NINGHUI LI, Purdue University
HIMANSHU NEEMA, Vanderbilt University
DEAN O, Government Communications Headquarteres
ALEX POTANIN, Victoria University of Wellington
ANTONIO ROQUE, Tufts University
ADAM TAGERT, National Security Agency
BHAVANI THURAISINGHAM, University of Texas at Dallas
PETER VOLGYESI, Vanderbilt University
JINPENG WEI, University of North Carolina Charlotte
QUANYAN ZHU, New York University

ORGANIZING COMMITTEE:

SPECIAL WORKSHOP CHAIR:
TRAVIS BREAUX, Carnegie Mellon University

PUBLICATIONS CHAIR:
ZHENKAI ZHANG, Vanderbilt University

LOCAL ARRANGEMENTS:
KATIE DEY, Vanderbilt University

NSA LIASONS:
HEATHER LUCAS, ADAM TAGERT, and **TIM THIMMESCH**

GRAPHIC DESIGN:
AMY KARNS, Vanderbilt University

2019HoTSoSBooklet_revised.indd 6 3/18/19 10:48 AM

AGENDA

Monday, April 1

1600 - 1730 **Tutorial: Game Theory for Cyber Deception** *Wyatt Rotunda*

Quanyan Zhu, New York University

1800 - 1930 **Evening Reception at The Wyatt Center Lobby**

Tuesday, April 2

0730 - 0830 **Breakfast | Registration** *(open until 1730)*

SESSION 1 *Wyatt Rotunda*

0830 - 0845 **Welcome and Introduction**

Symposium Chairs: *Xenofon Koutsoukos, Alvaro Cardenas, and Ehab Al-Shaer*

NSA Opening Remarks

0845 - 0945 **Keynote: Accountability in Computing**

Rebecca Wright, Barnard College and Rutgers University

0945 - 1000 **Break**

SESSION 2 *Wyatt Rotunda*

1000 - 1030 **BEEER: Distributed Record and Replay for Medical Devices in Hospital Operating Rooms**

**Avesta Hojjati, *Yunhui Long, †Soteris Demetriou, and *Carl A. Gunter*

*University of Illinois at Urbana-Champaign,

†Imperial College London

1030 - 1100 **Limitations on Observability of Effects in Cyber-Physical Systems**

Suresh K Damodaran and Paul Rowe

MITRE

1100 - 1130 **Integrated Data Space Randomization and Control Reconfiguration for Securing Cyber-Physical Systems**

Bradley Potteiger, Zhenkai Zhang and Xenofon Koutsoukos

Vanderbilt University

2019HoTSoSBooklet_revised.indd 7 3/18/19 10:48 AM

AGENDA

1130 - 1245 **Lunch**

SESSION 3 *Wyatt Rotunda*

1245 - 1415 **PANEL: Are There Fundamental Truths in Cybersecurity?**
Moderator: *Adam Tagert*
Panelists:
Tiffany Bao, Arizona State University
Dan Geer, In-Q-Tel
Trent Jaeger, The Pennsylvania State University
Jonathan Spring, University College, London

1415 - 1500 **Posters and Break**

SESSION 4 *Wyatt Rotunda*

1500 - 1730 **Special Workshop Session**

Uninformed but Unconcerned: Privacy Attitudes of Smart Speaker Users
**Nathan Malkin, *†Serge Egelman,*
*UC Berkeley, †International Computer Science Institute

The Impact of Ad-Blockers on Consumer Behavior: A Lab Experiment
**Alisa Frik, †Amelia Haviland, and †Alessandro Acquisti*
*International Computer Science Institute
†Heinz College - Carnegie Mellon University

Is Mobile App Tracking Really Anonymous and Aggregative?
**Xueling Zhang, *Xiaoyin Wang, *Mitra Bokaei Hosseini, *John Heaps, *Xue Qin, *Jarred Deeley, †Travis Breaux, and *Jianwei Niu*
*UT San Antonio, †Carnegie Mellon University

1730 **Adjourn**

1830 - 2100 **Dinner at the The Bridge Building**

Wednesday, April 3

0800 - 0830 **Breakfast | Registration** *(open until 1630)*

SESSION 5 *Wyatt Rotunda*

0800 - 0830 **Keynote: Toward a Science of Cyberdeception**
Kevin Hamlen, UT Dallas

0930 - 1015 **Posters and Break**

2019HoTSoSBooklet_revised.indd 8 3/18/19 10:48 AM

AGENDA

SESSION 6

Wyatt Rotunda

1015 - 1045 **How Shall We Play a Game? A Game-theoretical Model for Cyber-warfare Games**

Tiffany Bao, Arizona State University

6th Annual Best Scientific Cybersecurity Paper Competition Winner

1045 - 1115 **Game Theory for Adaptive Defensive Cyber Deception**

**Kimberly Ferguson-Walter, †Sunny Fugate, †Justin Mauger and †Maxine Major*

*Department of Defense, †Space and Naval Warfare Systems Center, Pacific

1115 - 1145 **Situated Information Flow Theory**

Sebastian Benthall, New York University

1145 - 1245 **Lunch**

SESSION 7

Wyatt Rotunda

1245 - 1345 **Keynote: The Science of Attack Surfaces and Its Applications**

Trent Jaeger, The Pennsylvania State University

1345 - 1500 **Works-in-Progress/ Works-already-Published Session** *(12 mins each)*

A Graph-Based Analysis of Industrial Control Systems Network Traffic

Imani Palmer, Shane McFly, and Edmond Rogers
University of Illinois at Urbana-Champaign

A Multidimensional Multilevel Model for Smart Environment

Amir Modarresi, John Symons, and James Sterbenz
The University of Kansas

Attacks on Electricity Markets

Carlos Barreto and Xenofon Koutsoukos
Vanderbilt University

Ethics in Norm-Aware Agents

**Nirav Ajmeri, *Hui Guo, †Pradeep Kumar Murukannaiah, and *Munindar Singh,* *North Carolina State University, †Rochester Institute of Technology

Search Prevention using Captchas against Web Search Engine: A Proof of Concept

Luke Sample and Donghoon Kim, Arkansas State University

The Tularosa Study: An Experimental Design and Implementation to Quantify the Effectiveness of Cyber Deception

**Kimberly Ferguson-Walter, *Temmie Shade, *Andrew Rogers, †Elizabeth Niedbala, ‡Michael Trumbo, ‡Kevin Nauer, ‡Aaron Jones, ‡Angela Combs, and ‡Robert Abbott*
*Department of Defense, †Texas Tech University, ‡Sandia National Laboratories

2019HoTSoSBooklet_revised.indd 9 3/18/19 10:48 AM

AGENDA

1500 - 1515 **Break**

SESSION 8 *Wyatt Rotunda*

1515 - 1545 **A Copland Attestation Manager**

Adam Petz and Perry Alexander
The University of Kansas

1545 - 1615 **Browser Fingerprinting using Combinatorial Sequence Testing**

**Bernhard Garn, *Dimitris E. Simos, †Stefan Zauner, ‡Rick Kuhn and ‡Raghu Kacker*

*SBA Research, †FH Campus Wien, ‡National Institute of Standards and Technology

1615 - 1630 **Announcement of Winning Paper and Winning Poster**

Adam Tagert

HotSoS 2020 Announcement

Perry Alexander, The University of Kansas

Closing Remarks

Xenofon Koutsoukos

SYMPOSIUM ADJOURNED

2019HoTSoSBooklet_revised.indd 10 3/18/19 10:48 AM

KEYNOTE



REBECCA WRIGHT
Bernard College & Rutgers University

Accountability in Computing

Accountability is used often in describing computer-security mechanisms that complement preventive security, but it lacks a precise, agreed-upon definition. Here, we argue for the need for accountability in computing in a variety of settings, categorize some of the many ways in which this term is used, and propose a punishment-focused view of "accountability." We formalize our view in a utility-theoretic way and then use this to reason about accountability in computing systems. We also survey mechanisms providing various senses of accountability as well as other approaches to reasoning about accountability-related properties.

Rebecca Wright is the Druckenmiller Professor of Computer Science and Director of the Vagelos Computational Science Center at Barnard. She is currently on leave from Rutgers University, where she served as director of the DIMACS center and as the founding faculty advisor for the Douglass-SAS-DIMACS Computer Science Living-Learning Community for first-year Rutgers women in Computer Science. Wright's research is primarily in the area of information security, including privacy, applied cryptography, foundations of computer security, and fault-tolerant distributed computing. Wright serves as an editor of the International Journal of Information and Computer Security and of the Transactions on Data Privacy, and is a member of the board of the Computer Research Association's Committee on the Status of Women in Computing Research (CRA-W). She received a Ph.D. in Computer Science from Yale University, a B.A. from Columbia University, and an honorary M.E. from Stevens Institute of Technology. She is a Fellow of the IEEE and a Distinguished Member of the ACM.

2019HoTSoSBooklet_revised.indd 11 3/18/19 10:48 AM

KEYNOTE



KEVIN HAMLEN
University of Texas at Dallas

Toward a Science of Cyberdeception

For decades, secure software development methodologies have focused mainly on keeping attackers out---by eliminating software vulnerabilities or by detecting and mitigating their exploitation. But aggressively keeping detected attackers out has an unfortunate side-effect: it denies defenders critical threat intelligence that is only observable from longer, more substantive adversarial interactions. Software cyberdeceptions, such as honeypotting, are an important avenue for gathering this prized threat data, but are often designed and deployed unscientifically, and with services that attract and deceive only weak threats whose TTPs are less valuable to defenders than those of skillful adversaries.

In this talk, I will argue that a more rigorous science of software cyberdeception has the potential to offer many powerful advantages for cyberdefense, and might even be considered an "easy win" relative to traditional strategies that are unscalable or provably hard by comparison. However, it requires a deeply interdisciplinary approach that forces us to rethink how we approach certain aspects of software engineering, testing and evaluation, economics of security, human-computer interaction, software virtualization, and risk management.

Dr. Kevin Hamlen is a Eugene McDermott Professor of Computer Science at the University of Texas at Dallas, and director of the Software Languages Security Lab (SL)^2. His research on software binary analysis, formal methods approaches to security, malware active defense, and software cyberdeception has received numerous best paper awards, including twice receiving an NYU-Poly Best Applied Security Paper of the Year award, and has been spotlighted by thousands of news headlines worldwide, including in The Economist and New Scientist. He is the recipient of both the NSF CAREER and AFOSR Young Investigator Awards, as well as support from Navy, NSA, Army, and DARPA. Dr. Hamlen received his PhD from Cornell University and his BS from Carnegie Mellon University, where he received the Allen Newell Award for his research on proof-carrying code.

2019HoTSoSBooklet_revised.indd 12 3/18/19 10:48 AM

KEYNOTE



TRENT JAEGER
The Pennsylvania State University

The Science of Attack Surfaces and Its Applications

Michael Howard of Microsoft identified the principle of an attack surface as the number of "attack opportunities" that a program or system makes available to adversaries. Often adversaries take advantage of undefensed opportunities to launch exploits, so understanding attack surfaces could be valuable in preventing vulnerabilities proactively. In this talk, I will discuss various research endeavors that we and other researchers have explored in computing, representing, and reasoning about attack surfaces to identify where and how to augment defenses. Examples include the methods to use attack surface to compare relative security, identify vulnerabilities in file system access, compute exploits within programs, etc. Also, we will compare attack surfaces to alternative representations, such as attack graphs. We will discuss methods for computing attack surfaces in systems and for programs and challenges in applying the attack surface metric more broadly for developing intrusion detection techniques.

Trent Jaeger is a Professor in the Computer Science and Engineering Department at The Pennsylvania State University and the Co-Director of the Systems and Internet Infrastructure Security (SIIS) Lab. Trent's research interests include operating systems security and the application of programming language techniques to software security. He has published over 125 refereed research papers and is the author of the book "Operating Systems Security," which examines the principles of designs for secure operating systems. Trent has made a variety of contributions to open source systems security, particularly to the Linux Security Modules framework, Linux Integrity Measurement framework, and recently, security namespaces for Linux containers. He was Chair of the ACM Special Interest Group on Security, Audit, and Control (ACM SIGSAC) from 2013-2017, is on the steering committees of two of the major computer security research conferences (ACM CCS and NDSS, as Chair), and is the Consortium Lead for the Army Research Lab's Collaborative Research Alliance devoted to the science of security. Trent has an M.S. and a Ph.D. from the University of Michigan, Ann Arbor in Computer Science and Engineering, respectively, and spent nine years at IBM Research prior to joining Penn State.

2019HoTSoSBooklet_revised.indd 13 3/18/19 10:48 AM

POSTER LISTING

A Bird's Eye View of Knowledge Needs Related to Penetration Testing
Akond Rahman and Laurie Williams
North Carolina State University

A Change Would Do You Good: GA-based Approach for Hiding Data in Program Executables
Ryan Gabrys and Luis Martinez
Naval Information Warfare Center (NIWC) Pacific

A Formal Verification of Mutation-based Moving Target Defense
Muhammad Abdul Basit Ur Rahim, Qi Duan, and Ehab Al-Shaer
University of North Carolina at Charlotte

A New Metric to Compare Anomaly Detection Algorithms in Cyber-Physical Systems
**Jairo Giraldo and +Alvaro A. Cardenas*
*University of Texas at Dallas, +University of California Santa Cruz

A Synopsis of Static Analysis Alerts On Open Source Software
Nasif Imtiaz and Laurie Williams
North Carolina State University

CLIPS/ActiveSDN for Automated and Safe Cybersecurity Course-of-Actions Orchestration
Md Mazharul Islam, Ehab Al-Shaer, Ashutosh Dutta, and Mohammed Noraden Alsaleh
University of North Carolina at Charlotte

Cyber Defense Matrix- A New Model for Optimal Composition of Cybersecurity Controls for Constructing Resilient Risk Mitigation
Ashutosh Dutta and Ehab Al-Shaer
University of North Carolina at Charlotte

Design and Simulation Platform for Evaluation of Grid Distribution System and Transactive Energy
**Ryan Brunner, *Sang Keun Oh, *Jesse Ramirez, *Paul Houck, *Nathaniel Stickney, and +Raymond Blaine*
*United States Military Academy, +Cyber Research Center

Design for an Educational Cyber Range
**Ryan Brunner, *Sang Keun Oh, *Jesse Ramirez, *Paul Houck, *Nathaniel Stickney, and +Raymond Blaine*
*United States Military Academy, +Cyber Research Center

Designing a Raspberry Pi Sensor Network for Remote Observation of Wildlife
Brian Curtin, Rachelle H. David, Emmet D. Dunham, Cullen D. Johnson, Nikhil Shyamkumar, Thomas A. Babbitt, Suzanne J. Matthews
United States Military Academy

Exploring RNNs for Analyzing Zeek HTTP Data
**Daniel Andrews, *Jennifer Behn, *Danielle Jaksha, *Jinwon Seo, *Madeleine Schneider, *James Yoon, *Suzanne J. Matthews, +Rajeev Agrawal, *Alexander S. Mentis*
*United States Military Academy, +U.S. Army E.R.D.C.

2019HoTSoSBooklet_revised.indd 14 3/18/19 10:48 AM

POSTER LISTING

IoCDigger: Extracting Indicators of Compromise (IoCs) from Social Media
Reginald Harper, Amirreza Niakanlahiji, and Bei-Tseng Chu
University of North Carolina at Charlotte

Learning APT Chains from Cyber Threat Intelligence
Phuong Cao, Ghaith Husari, Ehab Al-Shaer, Ruhani Faiheem Rahman, and Bill Chu
University of North Carolina at Charlotte

Load Forecasting with Adversarial Attacks in Power Systems Using DeepForge
**Xingyu Zhou, *Yi Li, *Carlos Barreto, +Peter Volgyesi, +Xenofon Koutsoukos*
*Vanderbilt University, +Vanderbilt University, Institute for Software Integrated Systems

Measures and Metrics for the Enforcement of Critical Security Controls: A Case Study of Boundary Defense
Mohiuddin Ahmed and Ehab Al-Shaer
University of North Carolina at Charlotte

Simulation Based Evaluation of Security and Resilience in Railway Infrastructure
Bradley Potteiger, Hamzah Abdel-Aziz, Himanshu Neema, Xenofon Koutsoukos
Vanderbilt University

Taming Web Views in the Detection of Android Privacy Leaks
**Xue Qin, *Robert Neuhaus, *Diego Gonzales, *Xiaoyin Wang, +Travis Breaux, *Jianwei Niu*
*The University of Texas at San Antonio, +Carnegie Mellon University

ThreatZoom: Neural Network for Automated Vulnerability Mitigation
Ehsan Aghaei and Ehab Al-shaer
University of North Carolina-Charlotte

Toward a Reliability Measurement Framework Automated Using Deep Learning
**John Heaps, *Xiaoyin Wang, +Travis Breaux, *Jianwei Niu*
*The University of Texas at San Antonio, +Carnegie Mellon University

Towards an Understanding of Resilience with Complex Networks
Francisco Pipa and John Symons
University of Kansas

TRACTION: An Infrastructure for TRusted Alert sharing and Collaborative mitigaTION
**Keywhan Chung, *Phuong Cao, *Yuming Wu, *Zbigniew T. Kalbarczyk, *Ravishankar K. Iyer, +Alexander Withers*
*University of Illinois at Urbana-Champaign,
+National Center for Supercomputing Applications

2019HoTSoSBooklet_revised.indd 15 3/18/19 10:48 AM

SOS OUTREACH

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.

https://cps-vo.org/group/sos/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.

https://cps-vo.org/group/SoS/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.

2019HoTSoSBooklet_revised.indd 16 3/18/19 10:48 AM

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 five 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 Five 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.

2019HoTSoSBooklet_revised.indd 17 3/18/19 10:48 AM

RESTAURANTS

RESTAURANTS NEAR EMBASSY SUITES MIDTOWN

in order by distance from hotel

Hattie B's Hot Chicken
American Restaurant
112 19th Ave S
(615) 678-4794

Tavern
American Restaurant
1904 Broadway
(615) 320-8580

DeSano Pizza Bakery
American Restaurant
115 16th Ave S
(615) 953-1168

Le Sel
French Cuisine
1922 Adelicia St
(615) 490-8550

Hopdoddy Burger Bar
American Restaurant
1805 21st Ave S #100
(615) 823-2337

Puckett's Grocery
American Restaurant
500 Church St
(615) 770-2772

Martin's BBQ
American Restaurant
410 4th Ave S
(615) 288-0880

The Farm House
American Restaurant
210 Almond St
(615) 522-0688

Midtown Cafe
American Restaurant
102 19th Ave S
(615) 320-7176

Americano Free Style Tapas
Spanish Restaurant
1720 West End Ave
(615) 321-2209

Amerigo
Italian Restaurant
1920 W End Ave
(615) 320-1740

J. Alexander's Redlands Grill
American Restaurant
2609 West End Ave
(615) 340-9901

Otaku Ramen
Ramen Restaurant
1104 Division Street
(615) 942-8281

Merchants Restaurant
American Restaurant
401 Broadway
(615) 254-1892

The Southern Steak and Oyster
American Restaurant
150 3rd Ave S #110
(615) 724-1762

Urban Grub
American Restaurant
2506 12th Ave S
(615) 679-9342

2019HoTSoSBooklet_revised.indd 18 3/18/19 10:48 AM

NOTES

2019HoTSoSBooklet_revised.indd 19 3/18/19 10:48 AM

NOTES

2019HoTSoSBooklet_revised.indd 20 3/18/19 10:48 AM

sos-vo.org

