

5TH ANNUAL
HOT TOPICS *in the* **SCIENCE OF SECURITY**

APRIL 10-11, 2018 | RALEIGH, NORTH CAROLINA

http://hot-sos.com





hosted by:

NORTH CAROLINA STATE UNIVERSITY

5TH ANNUAL

HOT TOPICS in the SCIENCE OF SECURITY

April 10-11, 2018 | Raleigh, NC

http://hot-sos.com

WELCOME

Welcome to the 5th 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, an industry track, and a poster session.

As in previous instances, 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 including researchers and skilled practitioners from diverse disciplines that is focused around the advancement of scientific methods as applied to cybersecurity.

As in previous years, HotSoS 2018 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.

This year, HotSoS also solicited papers focusing on the above problems and having specific applications to privacy, broadly construed, and security of cyber-physical systems.

Submissions were subject to a rigorous reviewing process, and ultimately 9 out of 17 submitted papers were accepted. In addition, the program includes two tutorials.

We invited four invited speakers. We are grateful to Steve Lipner, Ari Schwartz, David Burke, and Ravi Sandhu for giving keynote lectures at HoTSoS.

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. Finally, we acknowledge the NSA for their continual support of the science of security community. We would also like to thank David Wright for his diligent efforts as local arrangements chair. Katie and David pulled together the logistics that made HoTSoS possible.

Munindar Singh and Laurie Williams, Co-General Chairs
Rick Kuhn and Tao Xie, Co-Program Chairs

TABLE OF CONTENTS

Welcome 2

Table of Contents 3

Welcome 4

General Information 5

Organization 6

Program Agenda 8

Keynote Presenters 11

Poster Presentations 15

Science of Security Program 16

Notes 18

ORGANIZATION

GENERAL CO-CHAIRS:



MUNINDAR SINGH is a full professor in the department of computer science at North Carolina State University. Munindar's research interests include multiagent systems and service-oriented computing, wherein he addresses the challenges of trust, service discovery, and business processes and protocols in large-scale open environments. Munindar is a co-director of the NCSU Science of Security Lablet.



LAURIE WILLIAMS is the Interim Department Head of Computer Science and a Professor in the Computer Science Department of the College of Engineering at North Carolina State University (NCSU). Laurie is a co-director of the NCSU Science of Security Lablet. Laurie's research focuses on software security particularly in relation to healthcare IT; agile software development practices and processes, particularly continuous deployment; and software reliability, software testing and analysis.

PROGRAM CO-CHAIRS:



RICK KUHN is a computer scientist in the Computer Security Division of the National Institute of Standards and Technology. He has authored two books and more than 100 conference or journal publications on information security, empirical studies of software failure, and software assurance, and is a senior member of the Institute of Electrical and Electronics Engineers (IEEE). He co-developed the role based access control model (RBAC) used throughout industry and led the effort that established RBAC as an ANSI standard. Previously he served as Program Manager for the Committee on Applications and Technology of the President's Information Infrastructure Task Force and as manager of the Software Quality Group at NIST.



TAO XIE is a Professor and Willett Faculty Scholar in the Department of Computer Science at the University of Illinois at Urbana-Champaign, USA. He worked as a visiting researcher at Microsoft Research. His research interests are in software engineering, focusing on software testing, program analysis, software analytics, software security, and educational software engineering. He received a 2016 Microsoft Research Outstanding Collaborators Award, a 2014 Google Faculty Research Award, 2008, 2009, and 2010 IBM Faculty Awards. He is an ACM Distinguished Speaker and an IEEE Computer Society Distinguished Visitor. He is an ACM Distinguished Scientist. His homepage is at http://taoxie.cs.illinois.edu.

ORGANIZATION

INDUSTRY CO-CHAIRS:

NIKOLA VOUK, McKinsey & Co.
JEREMY MAXWELL, Allscripts

FINANCE CHAIR

ÖZGÜR KAFALI, University of Kent, UK

PUBLICITY CHAIR:

KATIE DEY, Vanderbilt University

LOCAL ARRANGEMENTS:

DAVID WRIGHT, North Carolina State University

NSA LIASONS:

HEATHER LUCAS, and **TIM THIMMESCH**

GRAPHIC DESIGN:

AMY KARNS, Vanderbilt University

SPONSORS & DONORS:

Sponsored by
National Security Agency

Organized in cooperation with
ACM SIGSAG

Hosted by
North Carolina State University

PLATINUM DONOR: Merck
http://www.merck.com

We would especially like to thank our platinum donor, Merck, for their generous contribution which enabled the participation of many of the graduate students.

ORGANIZATION

PROGRAM COMMITTEE:

JONATHAN ALDRICH, Carnegie Mellon University
HOMA ALEMZADEH, University of Virginia
JEAN CAMP, Indiana University
AMIT CHOPRA, Lancaster University, UK
DANIELA CRUZES, SINTEF
MICHEL CUKIER, University of Maryland, College Park
CHRISTOPHER GATES, Symantec
VINCENT HU, NIST
LIMIN JIA, Carnegie Mellon University
ÖZGÜR KAFALı, University of Kent, UK
SNEHA KASERA, University of Utah
JONATHAN KATZ, University of Maryland, College Park
NADIN KOKCIYAN, King's College London, UK
CONSTANTINOS KOLIAS, George Mason University
CARL LANDWEHR, George Washington University
YVES LE TRAON, University of Luxembourg, Luxembourg
EMIL LUPU, Imperial College, UK
AARON MASSEY, University of Maryland, Baltimore County
SAYAN MITRA, University of Illinois at Urbana-Champaign
PRADEEP KUMAR MURUKANNAIAH, Rochester Institute of Tech.
CHRISTOPHER OEHMEN, Pacific Northwest National Laboratory
PETE ROTELLA, Cisco
SEAN SMITH, Dartmouth College
ADAM TAGERT, National Security Agency
CLAIRE VISHIK, Intel Corporation, UK
JEFF VOAS, NIST
TIM WEIL, Scram Systems
DAVID A. WHEELER, IDA
REBECCA WRIGHT, Rutgers University
DINGHAO WU, Pennsylvania State University
XUSHENG XIAO, Case Western Reserve University
ZHI XU, Palo Alto Networks
DANFENG YAO, Virginia Tech
TING YU, Qatar Computing Research Institute, Qatar

Tuesday, April 4

AGENDA

0730 - 1700 **Registration**

SESSION 1

0830 - 0900 **Welcome and Introduction**

Symposium Co-Chairs:
Laurie Williams and Munindar Singh

Opening Remarks

George Coker, National Security Agency

0900 - 1000 **Keynote: Foundational Cybersecurity Research: Report of a Study by NASEM**

Steve Lipner, Executive Director, SAFECode

1000 - 1045 **Poster Session and Break**

SESSION 2 *(Dual Track)*
PAPER TRACK: Vulnerabilities & Detection

1045 - 1110 **Robustness of Deep Autoencoder in Intrusion Detection under Adversarial Contamination**

Pooria Madani, Natalija Vlajic
University of York

1110 - 1135 **Understanding the Challenges to Adoption of the Microsoft Elevation of Privilege Game**

*†Inger Anne Tøndel, *Tosin Daniel Oyetoyan, *Martin Gilje Jaatun, and *Daniela S. Cruzes*
*Norwegian University of Science and Technology, †SINTEF Digital

1135 - 1200 **Reinventing the Privilege Drop: How Principled Preservation of Programmer Intent Would Prevent Security Bugs**

*†Ira Ray Jenkins, †Sergey Bratus, †Sean Smith, and *Maxwell Koo*
†Dartmouth College, *Narf Industries

SESSION 2 *(Dual Track)*
TUTORIAL/INDUSTRY TRACK

1045 - 1200 **Tutorial: Combinational Security Testing Course**

*†Dimitris Simo, *Rick Kuhn*
†SBA Research, *NIST
(until noon)

1200 - 1315 **Lunch**

Presentation: Building a Virtually Air-gapped Secure Environment in AWS

Erkang Zheng, Phil Gates-Idem, and Matt Lavin
LIfeOmic, Inc.

SESSION 3

1315 - 1415 **Keynote: You've Got a Vuln, I've Got a Vuln, Everybody's Got a Vuln**
Ari Schwartz, Venable LLP

1415 - 1515 **Panel: Cybersecurity Framework Practitioners**
Moderator: *Nikola Vouk,* Independent
Jeremy Maxwell, Allscripts
Andrew Porter, Merck
Alex Rogozhin, BB&T
Greg Witte, G2

1515 - 1600 **Poster Session and Break**

SESSION 4 *(Dual Track)*
PAPER TRACK: Secure Construction

1600 - 1625 **SecureMR: Secure MapReduce Computation Using Homomorphic Encryption and Program Partitioning**
*†Yao Dong, †Ana Milanova, and *Julian Dolby*
†Rensselaer Polytechnic Institute, *IBM

1625 - 1650 **Integrated Instruction Set Randomization and Control Reconfiguration for Securing Cyber-Physical Systems**
Bradley Potteiger, Zhenkai Zhang, and Xenofon Koutsoukos
Vanderbilt University

1650 - 1715 **Formal Verification of the W3C Web Authentication Protocol**
Iness Ben Guirat, Harry Halpin
†INSAT, *INRIA

SESSION 4 *(Dual Track)*
TUTORIAL/INDUSTRY TRACK

1600 - 1625 **DevSecOps: Security at the Speed of Software Development**
Larry Maccherone, Comcast

1625 - 1650 **HACSAW: A Trusted Framework for Cyber Situational Awareness**
Leslie Leonard, William Glodeck
Department of Defense

1650 - 1715 **Policy Governed Semi-Automated Security Checkpoints: Compliance as Code**
*†David Gonzalez, *Nikola Vouk*
†nearForm, *Independent

SESSION 5

1715 - 1800 **BREAK**

1800 **Shuttle to North Carolina Museum of Art**
(Meet in the Hotel Lobby - Don't be late!)

1830 - 2100 **Dinner - North Carolina Museum of Art**
2110 Blue Ridge Road, Raleigh, North Carolina 27607

Wednesday, April 5

0800 - 1530 **Registration**

SESSION 6

0900 - 1000 **Keynote: Cyber Security for Aviation Weapon Systems**
David Burke, NAVAIR Cyber Warfare Detachment

1000 - 1045 **Poster Session and Break**

SESSION 7 *(Dual Track)*
PAPER TRACK: Applications & Risk Evaluation

1045 - 1110 **Application of Capability-Based Cyber Risk Assessment Methodology to a Space System**
Martha McNeil, Thomas Llanso, and Dallas Pearson
Johns Hopkins University Applied Physics Laboratory

1110 - 1135 **Challenges and Approaches of Performing Canonical Action Research in Software Security**
*†Daniela S. Cruzes, †Martin Gilje Jaatun, and *Tosin Daniel Oyetoyan*
†SINTEF Digital, *Norwegian University of Science and Technology Laboratory

1135 - 1200 **Quantifying the Security Effectiveness of Firewalls and DMZs**
*†Huashan Chen, *Jin-Hee Cho, and †Shouhuai Xu*
†University of Texas at San Antonio, *Army Research Lab

SESSION 7 *(Dual Track)*
TUTORIAL/INDUSTRY TRACK

1045 - 1200 **Tutorial: CyberSecurity Framework**
Greg Witte, G2

1200 - 1315 **Lunch**

SESSION 8

1315 - 1345 **You Get Where You're Looking For: The Impact of Information Sources on Code Security**
Michelle Mazurek, University of Maryland
NSA Fifth Annual Best Scientific Cybersecurity Paper Competition Winner

1345 - 1415 **Microarchitectural Attacks: From the Basics to Arbitrary Read and Write Primitives without any Software Bugs**
Daniel Gruss, Graz University of Technology

1415 - 1430 **Break**

1430 - 1530 **Keynote: An Access Control Perspective on the Science of Security**
Ravi Sandhu, University of Texas at San Antonio

1530 **Announcement of Winning Paper and Winning Poster**
Carl Landwehr and Adam Tagert

Closing Remarks
Laurie Williams and Munindar Singh

KEYNOTE

Steve Lipner, Executive Director, SAFECode

"Foundational Cybersecurity Research: Report of a Study by NASEM"



Steven B. Lipner is the Executive Director of SAFECode, a non-profit industry organization dedicated to increasing trust in ICT products and services through the advancement of effective software assurance methods. He is also an Adjunct Professor of Computer Science in the Institute for Software Research, School of Computer Science at Carnegie Mellon University. Lipner retired in 2015 as Partner Director of Software Security at Microsoft where he was the creator and long-time leader of the Microsoft Security Development Lifecycle (SDL). He was also responsible for Microsoft's policies and strategies for security evaluation of products by governments, and for Microsoft's approach to supply chain security and product integrity. Before joining Microsoft, Lipner worked for several commercial vendors and government contractors as a researcher, consultant, engineering manager and general manager in computer and network security. He has written numerous technical papers on aspects of cybersecurity and served on nine National Academies committees. He holds twelve U.S. patents in computer and network security, and served two terms, a total of ten years, on the Information Security and Privacy Advisory Board. Lipner was elected in 2010 to the Information Systems Security Association Hall of Fame, in 2015 to the National Cybersecurity Hall of Fame, and in 2017 to the National Academy of Engineering.

ABSTRACT

What is a science of cybersecurity and what should the United States Government do to advance it? Between late 2012 and early 2015, a committee of the National Academies of Science, Engineering, and Medicine conducted a study of future research goals and directions for foundational science in cybersecurity. The committee sought to focus on opportunities where a fresh approach to the problem could prove fruitful and to consider gaps in the Federal research program in the science of cybersecurity. The committee identified four broad aims for cybersecurity research:

- Strengthen the scientific underpinnings of cybersecurity.
- Integrate the social, behavioral, and decision sciences in security science.
- Address engineering, operational, and life-cycle challenges in security science.

Support and sustain foundational research for security science.
The committee also recommended fostering institutional approaches and opportunities to improve security science, and a deliberate focus on incentivizing longer-term research efforts and infrastructure development. The committee's report is available on the NASEM website; this keynote will summarize the highlights of the report and elaborate on its key insights and contributions.



Ari Schwartz, Venable LLP

"You've Got a Vuln, I've Got a Vuln, Everybody's Got a Vuln"

Ari Schwartz is Venable's Managing Director of Cybersecurity Services. He directs the firm's cybersecurity consulting services, assisting organizations with understanding and developing risk management strategies, including implementation of the Cybersecurity Framework and other planning tools to help minimize risk. Previously, Mr. Schwartz served at the White House National Security Council, as Special Assistant to the President and Senior Director for Cybersecurity where he led legislative and policy outreach to businesses, trade groups and others. Before his work at the White House, Schwartz led the Department of Commerce's Internet Policy Task Force, worked at the National Institute of Standards and Technology, and served for twelve years at the Center for Democracy and Technology.

ABSTRACT

You've Got a Vuln, I've Got a Vuln, Everybody's Got a Vuln -- For many years, researchers and IT vendors have often been at odds trying to determine how to coordinate disclosure of newly found vulnerabilities in a way that gives researchers credit but ensures that a patch is ready to deploy before the vulnerability is made public. As coordination has been standardized and leaks of vulnerabilities found by governments have increased, new pressure has mounted on governments when they find vulnerabilities to share those with the vendor. Recently, this has also been reversed where IT vendors are expected to give governments a heads up before a patch is deployed. This complicated area of cybersecurity policy affects privacy, public safety and national security. Ari Schwartz, a former Special Assistant to the President for Cybersecurity, will discuss the current state of vulnerability disclosure policy and how it could affect government, academic and private security research.

KEYNOTE

David Burke, NAVAIR Cyber Warfare Detachment



"Cyber Security for Aviation Weapon Systems"

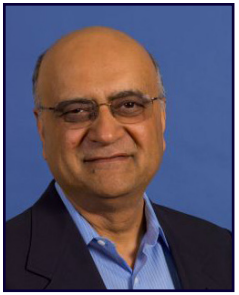
David Burke Ph.D., joined Naval Air Systems Command (NAVAIR) in 2010 as part of the Air Vehicle Modification & Instrumentation (AVMI) Division. Transitioning to support the Common Systems Integration (CSI) Office in 2011, he was tasked with improving the interoperability of Navy Unmanned Aerial Systems to better meet warfighter needs. As the technical lead for the CSI office Dr. Burke stood up and chaired the Naval UAS Interface Control Working Group (ICWG), a collaborative effort between the Navy and industry partners to develop Naval Interoperability Profiles (NIOPs). Dr. Burke was also heavily involved in NATO UAS Interoperability efforts including being the chairman for NATO STANAG 4586, the NATO UAS command and control standard. In 2014 NAVAIR Cyber Warfare Detachment (CWD) was established to guide NAVAIR in how to address emerging cyber threats to military weapons systems and Dr. Burke was chosen as its Technical Director, leading all technical development efforts. In June 2017, Dr. Burke was selected to a Senior Leadership (SL) position as Director of the CWD where he leads the development of overarching cyber warfare technical strategy, processes and capabilities within NAVAIR, and is the primary point of contact for technical exchanges both within NAVAIR and with external agencies.

Dr Burke graduated from North Carolina State in 2004 with BS degrees in Computer Engineering, Electrical Engineering, and Computer Science; in 2007 with MS degree in Computer Engineering; and in 2010 with Ph. D. in Aerospace Engineering. He also holds a graduate certificate in Cyber Warfare from Naval Postgraduate School.

ABSTRACT

Naval aviation is a complex mix of IT (information technologies) and OT (operational technologies) operating in some of the most challenging environments around the globe. Nearly all are heavily reliant on software and processing hardware. From military aircraft and missiles to support equipment and logistics/maintenance environments, these unique embedded systems, diverse missions and varying strategic environments make standard cybersecurity processes difficult to apply, and consequently drive new methods for establishing robust cybersecurity postures. The Naval Air Systems Command (NAVAIR) is the acquisition arm for Naval Aviation and responsible for the cybersecurity posture of these military systems. As such, NAVAIR is applying engineering rigor to the cybersecurity process. This talk discusses some of the general challenges and opportunities including where development science would be helpful for embedded aviation systems.

KEYNOTE



Ravi Sandhu, University of Texas at San Antonio

"An Access Control Perspective on the Science of Security"

Ravi Sandhu is Executive Director of the Institute for Cyber Security and Lead PI of the NSF Center for Security and Privacy Enhanced Cloud Computing at the University of Texas at San Antonio, where he holds the Lutcher Brown Endowed Chair. Previously he served on the faculty at George Mason University (1989-2007) and Ohio State University (1982-1989). He holds BTech and MTech degrees from IIT Bombay and Delhi, and MS and PhD degrees from Rutgers University. He is a Fellow of IEEE, ACM and AAAS, and has received numerous awards from IEEE, ACM, NSA, NIST and IFIP. A prolific and highly cited author, his research has been funded by NSF, NSA, NIST, DARPA, AFOSR, ONR, AFRL, ARO and private industry. His seminal papers on role-based access control established it as the dominant form of access control in practical systems. His numerous other models and mechanisms have also had considerable real-world impact. He served as Editor-in-Chief of the IEEE Transactions on Dependable and Secure Computing, and previously as founding Editor-in-Chief of ACM Transactions on Information and System Security. He was Chairman of ACM SIGSAC, and founded the ACM Conference on Computer and Communications Security, the ACM Symposium on Access Control Models and Technologies and the ACM Conference on Data and Application Security and Privacy. He has served as General Chair, Steering Committee Chair, Program Chair and Committee Member for numerous security conferences. He has consulted for leading industry and government organizations, and has lectured all over the world. He is an inventor on 30 security technology patents and has accumulated over 39,000 Google Scholar citations for his papers. At the Institute for Cyber Security his research projects include attribute-based access control, secure cloud computing, secure Internet of Things, secure information sharing, social computing security, and secure data provenance.

His web site is at www.profsandhu.com

ABSTRACT

Access Control is an essential component of cyber security since the emergence of the cyber discipline in the late 1960s. There can be no science of security without a strong influence from a science of access control. Ravi Sandhu will share his perspective on insights from his and his collaborators intensive research on the science of access control, and its significance for the bigger science of security.

POSTERS

A Comparative Analysis Of Manual Methods For Analyzing Security Requirements In Regulatory Documents
Sarah Elder and Anna Mattapallil | North Carolina State University

An Expert-based Bibliometric For A Science Of Security
Lindsey McGowen and Angela Stoica | North Carolina State University

Cryptography In A Post-quantum World
Katharine Ahrens | North Carolina State University

Detecting Monitor Compromise Using Evidential Reasoning
Uttam Thakore | University of Illinois at Urbana-Champaign

Ethics, Values And Personal Agents
Nirav Ajmeri | North Carolina State University

Exploring The Raspberry Pi For Data Summarization In Wireless Sensor Networks
Andres Alejos, Matthew Ball, Conner Eckert, Michael Ma, Hayden Ward, Peter Hanlon, and Suzanne J. Matthews | USMA

Hourglass-shaped Architecture For Model-based Development Of Safe And Secure Cyber-physical Systems
Muhammad Umer Tariq and Marilyn Wolf | GATech

How Bad Is It, Really? An Analysis Of Severity Scores For Vulnerabilities
Christopher Theisen and Laurie Williams | North Carolina State University

Indirect Cyber Attacks by Perturbation of Environment Control: A Data-Driven Attack Model
Keywhan Chung, Zbigniew T. Kalbarczyk, and Ravishankar K. Iyer
University of Illinois at Urbana-Champaign

Integrating Historical And Real-time Anomaly Detection To Create A More Resilient Smart Grid Architecture
Spencer Drakontaidis, Michael Stanchi, Gabriel Glazer, Madison Stark, Caleb Clay, Jason Hussey, Nick Barry, Aaron St. Leger, Suzanne J. Matthews
USMA

Investigating Tensorflow For Airport Facial Identification
Nikolay Shopov, Mingu Jeong, Evin Rude, Brennan Nessaralla, Scott Hutchison, Alexander Mentis, and Suzanne J. Matthews | USMA

Quantifying The Security Effectiveness Of Network Diversity
Huashan Chen and Shouhuai Xu | UT, San Antonio

Quantitative Underpinnings Of Secure Graceful Degradation
Ryan Wagner, David Garlan, and Matt Fredrikson | Carnegie Mellon University

Ransomware Research Framework
Dan Wolf and Don Goff | Cyber Pack Ventures, Inc.

Toward Extraction of Security Requirements from Text
**Hui Guo, +Ozgur Kafali, ++Anne-Liz Jeukeng, *Laurie Williams, *Munindar P. Singh*
*North Carolina State University, +University of Kent, ++University of Florida

Understanding Privacy Concerns Of Whatsapp Users In India
Jayati Dev, Sanchari Das, and Dr. L. Jean Camp
Indiana University Bloomington

Using Object Capabilities And Effects To Build An Authority-safe Module System
**Darya Melicher, *Yangqingwei Shi, +Valerie Zhao, ++Alex Potanin, *Jonathan Aldrich*
*Carnegie Mellon University, +Wellesley College, ++Victoria University of Wellington

What Proportion Of Vulnerabilities Can Be Attributed To Ordinary Coding Errors?
**Rick Kuhn, +Mohammad Raunak, and *Raghu Kacker*
*National Institute of Standards and Technology, +Loyola University

BEST SCIENTIFIC CYBER-SECURITY PAPER COMPETITION

TThe Best Scientific Cybersecurity Paper Competition is sponsored by the NSA RD 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

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.

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.

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 through the SoS Annual Report at http://sos-vo.org/annualreport

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 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, Kansas University, 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.

sos-vo.org

