Preface

The 5th Annual Symposium and Bootcamp on Hot Topics in the Science of Security (HotSoS) was held April 10-11, 2018 in Raleigh, NC. It included 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 dialog 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 focused on presentations and posters related to the hard problems of:

- **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 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 12 submissions (9 full paper submissions) 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 the 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 Laurie Williams Rick Kuhn Tao Xie
General Co-Chairs Program Co-Chairs

HoTSoS 2018

Raleigh, North Carolina, USA
April 10-11, 2018

Sponsored by *National Security Agency*

Organized in cooperation with *ACM SIGSAC*

General Co-Chairs

Munindar Singh, North Carolina State University
Laurie Williams, North Carolina State University

Program Co-Chairs

Rick Kuhn, National Institute of Standards and Technology
Tao Xie, University of Illinois Urbana-Champaign

Industry Co-Chairs

Nikola Vouk, McKinsey & Co.
Jeremy Maxwell, Allscripts

Finance Chair

Özgür Kafalı, 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

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
Ozgur Kafal	North Carolina State University
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 K. Murukannaiah	Rochester Institute of Technology
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

Table of Contents

Robustness of Deep Autoencoder in Intrusion Detection under Adversarial Contamination

Pooria Madani and Natalija Vlajic

University of York

Understanding the Challenges to Adoption of the Microsoft Elevation of Privilege Game

Inger Anne Tøndel[1], Tosin Daniel Oyetoyan[2], Martin Gilje Jaatun[2], and Daniela S. Cruzes[2]

[1]Norwegian University of Science and Technology, [2]SINTEF Digital

Reinventing the Privilege Drop: How Principled Preservation of Programmer Intent Would Prevent Security Bugs

Ira Ray Jenkins[1], Sergey Bratus[1], Sean Smith[1], and Maxwell Koo[2]

[1]Dartmouth College, [2]Narf Industries

SecureMR: Secure MapReduce Computation Using Homomorphic Encryption and Program Partitioning

Yao Dong[1], Ana Milanova[1], and Julian Dolby[2]

[1]Rensselaer Polytechnic Institute, [2]IBM

Integrated Instruction Set Randomization and Control Reconfiguration for Securing Cyber-Physical Systems

Bradley Potteiger, Zhenkai Zhang, and Xenofon Koutsoukos

Vanderbilt University

Formal Verification of the W3C Web Authentication Protocol

Iness Ben Guirat[1] and Harry Halpin[2]

[1]INSAT, [2]INRIA

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

Challenges and Approaches of Performing Canonical Action Research in Software Security

Daniela S. Cruzes[1], Martin Gilje Jaatun[1], and Tosin Daniel Oyetoyan[2]

[1]SINTEF Digital, [2]Norwegian University of Science and Technology

Quantifying the Security Effectiveness of Firewalls and DMZs

Huashan Chen[1], Jin-Hee Cho[2], and Shouhuai Xu[1]

[1]University of Texas at San Antonio, [2]Army Research Lab

Combinatorial Security Testing Course

Dimitris E. Simos[1], Rick Kuhn[2], Yu Lei[3], and Raghu Kacker[2]

[1]SBA Research, [2]National Institute of Standards and Technology, [3]University of Texas at Arlington

Building a Virtually Air-gapped Secure Environment in AWS

Erkang Zheng, Phil Gates-Idem, and Matt Lavin

LifeOmic, Inc.

HACSAW: A Trusted Framework for Cyber Situational Awareness

Leslie Leonard and William Glodek

Department of Defense (DoD) High Performance Computing Modernization Program (HPCMP)

Poster: A Comparative Analysis of Manual Methods for Analyzing Security Requirements in Regulatory Documents

Sarah Elder and Anna Mattapallil

North Carolina State University

Poster: An Expert-based Bibliometric for a Science of Security

Lindsey McGowen and Angela Stoica

North Carolina State University

Poster: Cryptography in a Post-Quantum World

Katharine Ahrens

North Carolina State University

Poster: Detecting Monitor Compromise Using Evidential Reasoning

Uttam Thakore

University of Illinois at Urbana-Champaign

Poster: Ethics, Values, and Personal Agents

Nirav Ajmeri

North Carolina State University

Poster: 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

Poster: Hourglass-shaped Architecture for Model-based Development of Safe and Secure Cyber-physical Systems

Muhammad Umer Tariq[1] and Marilyn Wolf[2]

[1]ProsumerGrid, Inc., [2]Georgia Institute of Technology

Poster: How Bad It It Really? An Analysis of Severity Scores for Vulnerabilities

Christopher Theisen and Laurie Williams

North Carolina State University

Poster: 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

Poster: 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, and Suzanne J. Matthews

USMA

Poster: Investigating Tensorflow for Airport Facial Identification

Nikolay Shopov, Mingu Jeong, Evin Rude, Brennan Nessaralla, Scott Hutchison, Alexander Mentis, and Suzanne J. Matthews

USMA

Poster: Quantifying the Security Effectiveness of Network Diversity

Huashan Chen and Shouhuai Xu

University of Texas at San Antonio

Poster: Quantitative Underpinnings of Secure Graceful Degradation

Ryan Wagner, David Garlan, and Matt Fredrikson

Carnegie Mellon University

Poster: A Ransomware Research Framework

Dan Wolf and Don Goff

Cyber Pack Ventures, Inc.

Poster: Toward Extraction of Security Requirements from Text

Hui Guo[1], Özgür Kafalı[2], Anne-Liz Jeukeng[3], Laurie Williams[1], and Munindar P. Singh[1]

[1]North Carolina State University, [2]University of Kent, [3]University of Florida

Poster: Understanding Privacy Concerns of WhatsApp Users in India

Jayati Dev, Sanchari Das, and L. Jean Camp

Indiana University Bloomington

Poster: Using Object Capabilities and Effects to Build an Authority-Safe Module System

Darya Melicher[1], Yangqingwei Shi[1], Valerie Zhao[2], Alex Potanin[3], and Jonathan Aldrich[1]

[1]Carnegie Mellon University, [2]Wellesley College, [3]Victoria University of Wellingon

Poster: What Proportion of Vulnerabilities Can Be Attributed to Ordinary Coding Errors?

Rick Kuhn[1], Mohammad Raunak[2], and Raghu Kacker[1]

[1]National Institute of Standards and Technology, [2]Loyola University